ΑΝΑΛΥΣΗ ΡΙΣΚΩΝ ΚΑΙ ΕΜΠΟΔΙΑ

ΕΙΣΑΓΩΓΗ

Ο κύριος στόχος του έργου MILEAGE είναι να δημιουργήσει έναν νέο και πιο ελκυστικό τρόπο για την προώθηση των ψηφιακών δεξιοτήτων των ηλικιακά μεγαλύτερων και του γραμματισμού τους στα μέσα ενημέρωσης και πληροφόρησης, ώστε να τους ενθαρρύνει να χρησιμοποιούν τα εργαλεία ΤΠΕ στην καθημερινή ζωή, ευαισθητοποιώντας τους σχετικά με τους ψηφιακούς κινδύνους και τον τρόπο αντιμετώπισής τους.

Πώς;

- Με μια έκθεση σχετικά με τους κινδύνους και τα εμπόδια που αντιμετωπίζουν οι ηλικιακά μεγαλύτεροι στο ψηφιακό περιβάλλον
- Με την ανάπτυξη εικονικών σεναρίων κινδύνου (παιχνίδι ρόλων)
- Με τη δημιουργία μικρο-μαθημάτων με επεξηγήσεις σχετικά με τους καθορισμένους κινδύνους
- Με τη σύνταξη ενός εγχειριδίου για εκπαιδευτές ενηλίκων με οδηγίες που υποστηρίζουν τις δραστηριότητες κατάρτισης (αποτέλεσμα προώθησης και ενημέρωσης).

Η παρούσα έκθεση για τους κινδύνους και τα εμπόδια παρουσιάζει τα κύρια μέσα κοινωνικής δικτύωσης, τα εργαλεία επικοινωνίας και άλλες πλατφόρμες που χρησιμοποιούνται ευρέως σήμερα. Περιγράφουμε συγκεκριμένα τους κινδύνους και τα ρίσκα που συνδέονται με αυτά : κάθε ζήτημα ή κίνδυνος αναλύεται και προσφέρεται μια λύση για την αντιμετώπισή του, παραθέτοντας επίσης τις ικανότητες που απαιτούνται και ενεργοποιούνται για τον σκοπό αυτό.

Το παρόν έγγραφο δημιουργήθηκε για να δώσει στους εκπαιδευτές, τους ηλικιακά μεγαλύτερους και το ευρύ κοινό ορισμένες πληροφορίες σχετικά με το ψηφιακό περιβάλλον, που αντιμετωπίζουν οι ηλικιακά μεγαλύτεροι στην καθημερινή τους ζωή, προσφέροντας ορισμένες συμβουλές για την ενίσχυση των ψηφιακών ικανοτήτων τους και της εμπιστοσύνης τους στον ψηφιακό κόσμο. Το έγγραφο αυτό θα καθοδηγήσει την ανάπτυξη του εκπαιδευτικού μας περιεχομένου και των σεναρίων κινδύνου, που δημιουργήθηκαν για την υποστήριξη του γραμματισμού στα μέσα ενημέρωσης και πληροφόρησης των ηλικιακά μεγαλύτερων.

MILEAGE

ΠΕΡΙΕΧΟΜΕΝΟ

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**WHATSAPP**
Γενικές πληροφορίες	Το WhatsApp είναι ένα δωρεάν πρόγραμμα επικοινωνίας για smartphone που μπορείτε να κατεβάσετε. Το WhatsApp στέλνει μηνύματα, φωτογραφίες, ήχο και βίντεο μέσω του διαδικτύου. Η υπηρεσία μοιάζει αρκετά με τις υπηρεσίες ανταλλαγής μηνυμάτων κειμένου- αλλά, επειδή το WhatsApp στέλνει μηνύματα μέσω του διαδικτύου, είναι πολύ λιγότερο δαπανηρό από τα γραπτά μηνύματα. Μπορείτε επίσης να χρησιμοποιήσετε το Whatsapp στον υπολογιστή σας. Επισκεφθείτε τον ιστότοπο του Whatsapp και κατεβάστε το πρόγραμμα για Mac ή Windows. Λόγω χαρακτηριστικών όπως η ομαδική συνομιλία, τα ηχητικά μηνύματα και η κοινή χρήση τοποθεσίας, είναι πολύ δημοφιλές στους νέους.
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο: **Ιδιωτικότητα, ακρίβεια, ιδιοκτησία, προσβασιμότητα, παραβίαση νόμων, πνευματικά δικαιώματα**	Απόρρητο Κλοπή προφίλ Καταγραφή των κλήσεων (εγκλήματα στον κυβερνοχώρο)
Εμπόδια/δυσκολίες για ενήλικες	Ρυθμίσεις απορρήτου.
Κίνδυνος των μέσων κοινωνικής δικτύωσης /εργαλείων για τους ενήλικες	Hackers Μη κρυπτογραφημένα αντίγραφα ασφαλείας
Λύσεις που μπορούμε να έχουμε	Ποτέ μην δίνετε τον κωδικό εγγραφής ή το PIN για την επαλήθευση δύο παραγόντων σε κανέναν άλλο. Δημιουργήστε έναν κωδικό για τη συσκευή σας. Παρακολουθήστε ποιος έχει πρόσβαση στο τηλέφωνό σας σε φυσικό επίπεδο. Γνώση των εφαρμογών και των ρυθμίσεών τους.

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**VIBER**
Γενικές πληροφορίες	Το Viber είναι μια δωρεάν εφαρμογή που επιτρέπει στους χρήστες να πραγματοποιούν δωρεάν κλήσεις, να στέλνουν μηνύματα κειμένου, φωτογραφίες και βίντεο σε άλλους χρήστες του Viber. Μπορεί να χρησιμοποιηθεί για τη σύνδεση με άτομα σε όλο τον κόσμο και λειτουργεί τόσο σε κινητά όσο και σε επιτραπέζιους υπολογιστές. Η εφαρμογή ανταλλαγής μηνυμάτων είχε 236 εκατομμύρια μηνιαίως ενεργούς χρήστες τον Φεβρουάριο του 2015. Η κοινοποίηση φωτογραφιών, το βίντεο και η ομαδική συνομιλία είναι δημοφιλή χαρακτηριστικά για τους νεαρούς καταναλωτές, παρόμοια με το WhatsApp.
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο: **Ιδιωτικότητα, ακρίβεια, ιδιοκτησία, προσβασιμότητα, παραβίαση νόμων, πνευματικά δικαιώματα**	Εκφοβισμός στον κυβερνοχώρο Απόρρητο Κλήσεις spam
Εμπόδια/δυσκολίες για ενήλικες	Ρυθμίσεις απορρήτου
Κίνδυνος των μέσων κοινωνικής δικτύωσης /εργαλείων στους ενήλικες	Hackers
Λύσεις που μπορούμε να έχουμε	Παρακολουθήστε ποιος έχει πρόσβαση στο τηλέφωνό σας σε φυσικό επίπεδο. Γνώση των εφαρμογών και των ρυθμίσεών τους. Αποκλεισμός ενός άλλου χρήστη στο Viber (Όταν λαμβάνετε ένα μήνυμα από μια άγνωστη επαφή.)

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**ΕΤΑΙΡΕΙΕΣ ΔΙΑΜΟΝΗΣ**
Γενικές πληροφορίες	Ως πάροχος καταλύματος νοείται οποιοσδήποτε παρέχει κατάλυμα έναντι αμοιβής ή φιλοξενεί περισσότερους από 5 αλλοδαπούς, εκτός από τις περιπτώσεις όπου ο αλλοδαπός και ο πάροχος μπορούν να θεωρηθούν ότι έχουν στενή σχέση. Παραδείγματα: Airbnb, Booking
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο: **Ιδιωτικότητα, ακρίβεια, ιδιοκτησία, προσβασιμότητα, παραβίαση νόμων, πνευματικά δικαιώματα**	Απάτες Παραπληροφόρηση/παραπλάνηση Απάτες με κάρτες
Εμπόδια/δυσκολίες για ενήλικες	Χρήση της τεχνολογίας για την κράτηση του καταλύματος Όροι και προϋποθέσεις που δεν είναι ορατά
Κίνδυνος των μέσων κοινωνικής δικτύωσης /εργαλείων στους ενήλικες	Χρήση της τεχνολογίας για την κράτηση του καταλύματος Όροι και προϋποθέσεις που δεν είναι ορατά Δεν είναι προσβάσιμο σε ηλικιακά μεγαλύτερους Απομόνωση
Λύσεις που μπορούμε να έχουμε	Οι δυσκολίες αυτές δεν σημαίνουν ότι η γήρανση είναι ανέφικτος ή ανεπιθύμητος στόχος, αλλά μάλλον ότι απαιτείται εκτεταμένος σχεδιασμός τόσο σε ατομικό όσο και σε κοινοτικό επίπεδο. Το πρώτο στάδιο είναι η ενημέρωση των επιχειρήσεων στέγασης σχετικά με τα οικονομικά και φυσικά προβλήματα που μπορεί να υπάρχουν, εάν παραμείνουν στην υπάρχουσα κατοικία τους, καθώς και τις διαθέσιμες λύσεις για την επίλυσή τους. Επίσης, σημαντική είναι και η διασφάλιση ότι οι τοπικές κυβερνήσεις είναι ενήμερες και προετοιμασμένες για τα ζητήματα που θα αντιμετωπίσουν οι ηλικιακά μεγαλύτεροι πολίτες τους.

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**ΕΤΑΙΡΕΙΕΣ ΠΤΗΣΕΩΝ**
Γενικές πληροφορίες	Οργανισμός που παρέχει αεροπορικές μεταφορές επιβατών και εμπορευμάτων.
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο: **Ιδιωτικότητα, ακρίβεια, ιδιοκτησία, προσβασιμότητα, παραβίαση νόμων, πνευματικά δικαιώματα**	Απάτες Παραπληροφόρηση Απάτες με κάρτες
Εμπόδια/δυσκολίες για ενήλικες	Χρήση της τεχνολογίας για την κράτηση της πτήσης
Κίνδυνος των μέσων κοινωνικής δικτύωσης /εργαλείων στους ενήλικες	Χρήση της τεχνολογίας για την κράτηση της πτήσης Όροι και προϋποθέσεις που δεν είναι ορατά Δεν είναι προσβάσιμο σε ηλικιακά μεγαλύτερους
Λύσεις που μπορούμε να έχουμε	Έγκαιρος προγραμματισμός Έρευνα για τα αεροπορικά ταξίδια και τη βοήθεια σε ηλικιακά μεγαλύτερους Διαχείριση στάθμευσης, για να ικανοποιήσετε τα προβλήματα κινητικότητας Προετοιμαστείτε για την ασφάλεια στο αεροδρόμιο Ελέγξτε για μειωμένα αεροπορικά εισιτήρια για ηλικιωμένους πολίτες Επιλέξτε τη σωστή **ώρα** πτήσης

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**ΠΛΑΤΦΟΡΜΕΣ ΓΝΩΡΙΜΙΩΝ**
Γενικές πληροφορίες	Οι πλατφόρμες γνωριμιών είναι ιστότοποι ή εφαρμογές που επιτρέπουν στα άτομα να επικοινωνούν, προκειμένου να αναπτύξουν μια σχέση. Η πρόσβαση σε αυτές τις τοποθεσίες απαιτεί συχνά από τους χρήστες να παρέχουν προσωπικές πληροφορίες όπως η ηλικία, το φύλο και η γεωγραφική θέση. Υπάρχουν εκατοντάδες διαφορετικές πλατφόρμες γνωριμιών. Μπορεί να είναι γενικευμένες ή εξειδικευμένες για ένα είδος σχέσης (ερωτική, φιλική) ή μια ομάδα μελών (θρησκευτική ή εθνική καταγωγή, σεξουαλικός προσανατολισμός και ηλικιακή ομάδα). Μερικές από τις πιο γνωστές πλατφόρμες είναι: Meetic, Tinder, Bumble, eDarling, Badoo, OkCupid κ.λπ. Παρόλο που οι περισσότερες πλατφόρμες γνωριμιών είναι δωρεάν, ορισμένες απαιτούν μηνιαία συνδρομή ή πληρωμή για πρόσθετα χαρακτηριστικά.
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο:	Απόρρητο Ψεύτικο προφίλ
Εμπόδια/δυσκολίες για ενήλικες	Η κύρια δυσκολία με τις πλατφόρμες γνωριμιών είναι η πρακτική χρήση αυτών των εργαλείων. Για να μπορέσουν να χρησιμοποιήσουν τέτοιες πλατφόρμες, οι ηλικιακά μεγαλύτεροι χρειάζονται αρκετά προχωρημένες γνώσεις ΤΠΕ. Για παράδειγμα, χρειάζονται μια διεύθυνση ηλεκτρονικού ταχυδρομείου για να συνδεθούν, γεγονός που σημαίνει ότι πρέπει να γνωρίζουν πώς να δημιουργούν μια διεύθυνση ηλεκτρονικού ταχυδρομείου και να τη χρησιμοποιούν. Η πλατφόρμα απαιτεί επίσης τη μεταφόρτωση φωτογραφιών, αλλά οι ηλικιακά μεγαλύτεροι δεν γνωρίζουν απαραίτητα πώς να το κάνουν.
Κίνδυνος των μέσων κοινωνικής δικτύωσης /εργαλείων στους ενήλικες	**Απόρρητο** Οι χρήστες μοιράζονται προσωπικές πληροφορίες σε αυτές τις πλατφόρμες, ελπίζοντας να βρουν ταίρι/ φίλο. Οι πληροφορίες που μοιράζονται περιλαμβάνουν φωτογραφίες τους, σεξουαλικό προσανατολισμό, ηλικία, θρησκεία, φύλο, τα χόμπι τους, αν έχουν παιδιά, ύψος κ.λπ. Επιπλέον, οι πλατφόρμες γνωριμιών προσφέρουν συχνά τη δυνατότητα σύνδεσης του προφίλ τους με τους λογαριασμούς τους στα μέσα κοινωνικής δικτύωσης, όπως το Facebook ή το Instagram, επιτρέποντας έτσι τον συγχρονισμό της εφαρμογής γνωριμιών με τα μέσα κοινωνικής δικτύωσης και την εμφάνιση προσωπικών πληροφοριών, όπως εικόνες, που θα φορτώνονται αυτόματα στο προφίλ γνωριμιών. Κάποτε υπάρχει παραβίαση της ασφάλειας, η οποία μπορεί να είναι ιδιαίτερα επιβλαβής για τους χρήστες, καθώς σε αυτές τις πλατφόρμες κοινοποιούνται ευαίσθητα δεδομένα. **Ψεύτικο προφίλ**

	Οι ηλικιακά μεγαλύτεροι που εγγράφονται σε πλατφόρμες γνωριμιών είναι συχνά μοναχικοί (διαζευγμένοι, χήροι) και ως εκ τούτου εναποθέτουν μεγάλες ελπίδες στη γνωριμία με έναν πιθανό σύντροφο. Ωστόσο, πολλά ψεύτικα προφίλ και απάτες συμβαίνουν σε αυτές τις πλατφόρμες. Οι άνθρωποι προσποιούνται ότι είναι κάτι που δεν είναι και εμπλέκονται σε μια συναισθηματική σχέση, για να δημιουργήσουν έναν δεσμό μόνο και μόνο για να αποσπάσουν χρήματα.
Λύσεις που μπορούμε να έχουμε	Πριν από τη δημιουργία λογαριασμού, οι χρήστες θα πρέπει να διαβάσουν την πολιτική απορρήτου και τους όρους χρήσης της πλατφόρμας. Είναι σημαντικό να κατανοήσουν τους όρους αυτούς όσο το δυνατόν περισσότερο, ώστε να είναι σε θέση να δώσουν τη συγκατάθεσή τους οικειοθελώς. Το catfishing (ψεύτικο προφίλ) μπορεί να προκαλέσει πραγματική ζημιά. Για να το αποτρέψουν, οι χρήστες μπορούν να ζητήσουν μια βιντεοκλήση με το άτομο με το οποίο μιλούν, προκειμένου να επαληθεύσουν ότι ταιριάζει με τις εικόνες στην ιστοσελίδα. Οι χρήστες μπορούν επίσης να χρησιμοποιήσουν εργαλεία όπως το Google Reverse Photo Search, για να επαληθεύσουν αν η φωτογραφία είναι πρωτότυπη ή αν προέρχεται από κάποιον άλλο. Το πιο σημαντικό είναι οι χρήστες να εμπιστεύονται το ένστικτό τους, εάν αισθάνονται ότι τους εξαπατούν και να προσέχουν με τις πληροφορίες που κοινοποιούν.

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**ONLINE ΤΡΑΠΕΖΕΣ**
Γενικές πληροφορίες	Οι ηλεκτρονικές τραπεζικές συναλλαγές είναι επίσης γνωστές ως Internet Banking, net banking ή e-banking. Πρόκειται για ένα ηλεκτρονικό σύστημα πληρωμών που επιτρέπει στον πελάτη μιας τράπεζας ή ενός χρηματοπιστωτικού ιδρύματος να πραγματοποιεί οικονομικές ή μη οικονομικές συναλλαγές online μέσω του διαδικτύου. Η υπηρεσία αυτή παρέχει ηλεκτρονική πρόσβαση σε όλες σχεδόν τις τραπεζικές υπηρεσίες που παραδοσιακά διατίθενται μέσω ενός τοπικού υποκαταστήματος, συμπεριλαμβανομένων των μεταφορών κεφαλαίων, των καταθέσεων και των ηλεκτρονικών πληρωμών λογαριασμών στους πελάτες. Μπορεί να έχει πρόσβαση κάθε άτομο που έχει εγγραφεί για ηλεκτρονικές συναλλαγές στην τράπεζα, που έχει ενεργό τραπεζικό λογαριασμό ή οποιοδήποτε χρηματοπιστωτικό ίδρυμα. Η ηλεκτρονική τράπεζα προσφέρει 24ωρη πρόσβαση στους λογαριασμούς των χρηστών καθημερινά. Είναι γρήγορη και βολική, επιτρέποντας την

	εκτέλεση συναλλαγών οπουδήποτε, οποτεδήποτε, από οποιαδήποτε συσκευή (υπολογιστή, smartphone, tablet) με πρόσβαση στο διαδίκτυο. Ορισμένες διαδικτυακές τράπεζες είναι παραδοσιακές τράπεζες που προσφέρουν επίσης επιλογή ηλεκτρονικών συναλλαγών, ενώ άλλες είναι μόνο διαδικτυακές και δεν έχουν φυσική παρουσία. Σύμφωνα με τη Eurostat, το 2020, ο μέσος όρος του πληθυσμού που χρησιμοποιεί ηλεκτρονικές τραπεζικές υπηρεσίες στην ΕΕ ήταν 60%. Στην Τσεχική Δημοκρατία έφτασε το 70%, αλλά στην Πολωνία ήταν μόνο 49%. Στην Ιταλία, το 86,8% των ατόμων που χρησιμοποιούν το διαδίκτυο χρησιμοποίησαν επίσης έναν δικτυακό τόπο ή μια εφαρμογή που σχετίζεται με τραπεζικές εργασίες. Στην τελευταία Παγκόσμια Έκθεση για τη Λιανική Τράπεζα, το 57% των καταναλωτών δηλώνει ότι προτιμά πλέον την τραπεζική δραστηριότητα μέσω διαδικτύου (online) από την παραδοσιακή συναλλαγή μέσω καταστημάτων. Και το 55% των καταναλωτών προτιμά πλέον τη χρήση τραπεζικών εφαρμογών μέσω κινητού τηλεφώνου για να παρακολουθεί τα οικονομικά του, από 47% που ήταν στην προ της πανδημίας εποχή.
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο: **Ιδιωτικότητα, ακρίβεια, ιδιοκτησία, προσβασιμότητα, παραβίαση νόμων, πνευματικά δικαιώματα**	Απόρρητο Εγκλήματα στον κυβερνοχώρο: κλοπή δεδομένων και απάτη.
Εμπόδια/δυσκολίες για ενήλικες	Οι δυσκολίες για τους ενήλικες μεγαλύτερης ηλικίας σχετίζονται με το θέμα του φόβου και της εμπιστοσύνης, καθώς και με την έλλειψη γνώσεων και καθοδήγησης σχετικά με τη χρήση του συστήματος ηλεκτρονικών συναλλαγών της τράπεζάς τους.
Κίνδυνος των κοινωνικών μέσων/εργαλείων στους ενήλικες	**Έλλειψη εμπιστοσύνης** Τα στοιχεία που συλλέχθηκαν από τους Casalo et al (2007) έδειξαν ότι η ασφάλεια και η ιδιωτικότητα του δικτυακού τόπου, η χρηστικότητα και η φήμη έχουν άμεση και σημαντική επίδραση στην εμπιστοσύνη των καταναλωτών στον δικτυακό τόπο χρηματοπιστωτικών υπηρεσιών. Παρατηρείται ότι η εμπιστοσύνη αποτελεί βασικό μεσολαβητικό παράγοντα στην ανάπτυξη της ηλεκτρονικής τραπεζικής δραστηριότητας. **Απάτη & κλοπή δεδομένων** Αυτός ο κίνδυνος είναι περισσότερο ένας κοινός φόβος παρά ένα συχνό πρόβλημα. Πράγματι, σύμφωνα με έρευνα που διεξήχθη το 2020 από τον Ευρωπαϊκό Οργανισμό Θεμελιωδών Δικαιωμάτων, το ένα τέταρτο των Ευρωπαίων (24%) ανησυχεί πολύ ότι τα στοιχεία του διαδικτυακού

	τραπεζικού λογαριασμού ή της κάρτας πληρωμών τους θα χρησιμοποιηθούν καταχρηστικά. Συνολικά, όμως, λιγότεροι από 1 στους 10 (8%) αντιμετώπισαν απάτη μέσω διαδικτυακών τραπεζικών συναλλαγών ή καρτών κατά τα πέντε έτη πριν από την έρευνα. Οι κάτοικοι του Ηνωμένου Βασιλείου (24%), της Γαλλίας (19%) και της Δανίας (15%) είναι πιο πιθανό να έχουν τέτοια εμπειρία. **Ασφάλεια** Ο κίνδυνος ασφάλειας συνδέεται με τον αυξανόμενο αριθμό απατηλών τραπεζικών ιστότοπων, με πλαστά μηνύματα ηλεκτρονικού ταχυδρομείου που υποτίθεται ότι αποστέλλονται από τράπεζες, με τη χρήση προγραμμάτων Trojan horse για τη σύλληψη των αναγνωριστικών ταυτότητας και των κωδικών πρόσβασης των χρηστών. Οι κίνδυνοι hacking (ένας χάκερ εισέρχεται σε έναν τραπεζικό λογαριασμό και κλέβει τα χρήματα) υπάρχουν επίσης, αν και είναι πολύ σπάνιοι. **Απόρρητο** Σύμφωνα με μελέτη του 2020 που δημοσιεύθηκε από την KPMG, το 87% των καταναλωτών δηλώνει ότι η προστασία των δεδομένων αποτελεί βασικό ανθρώπινο δικαίωμα. Ωστόσο, το 68% δηλώνει ότι δεν εμπιστεύεται τις εταιρείες να πωλούν ηθικά τα προσωπικά τους δεδομένα. **Παραβίαση δεδομένων και phishing (ηλεκτρονικό ψάρεμα)** Το 2020, οι ειδικοί ανακάλυψαν ένα πρόβλημα ασφαλείας σε μια τράπεζα, την 5η μεγαλύτερη τράπεζα στην Ευρώπη και την 16η μεγαλύτερη στον κόσμο. Το βελγικό υποκατάστημα της τράπεζας είχε μια λανθασμένη διαμόρφωση στο domain του ιστοτόπου της, επιτρέποντας τη λήψη των αρχείων της. Τα αρχεία αυτά περιείχαν ευαίσθητες πληροφορίες (όνομα, email, τηλέφωνο) που θα μπορούσαν να χρησιμοποιηθούν από χάκερς για την δυνητική εξυπηρέτηση των πελατών της τράπεζας. Το phishing είναι ένας τύπος επίθεσης που χρησιμοποιείται συχνά για την κλοπή των δεδομένων ενός χρήστη, συμπεριλαμβανομένων των στοιχείων σύνδεσης και των αριθμών πιστωτικών καρτών. Συμβαίνει όταν ένας χάκερ, προσποιούμενος ότι είναι μια έμπιστη οντότητα, εξαπατά το θύμα ώστε να ανοίξει ένα μήνυμα ηλεκτρονικού ταχυδρομείου, άμεσο μήνυμα ή γραπτό μήνυμα και κλέβει τις πληροφορίες του.
Λύσεις που μπορούμε να έχουμε	**Εκμάθηση χρήσης ηλεκτρονικής τράπεζας - σεμινάριο** Για καθοδήγηση στη χρήση του εργαλείου ηλεκτρονικής τράπεζάς σας, ζητήστε από τον τραπεζίτη σας το εκπαιδευτικό πρόγραμμα της τράπεζας. Κάθε τράπεζα έχει δημιουργήσει ένα τέτοιο. **Ασφάλεια & Ηλεκτρονική Τραπεζική Δραστηριότητα** Οι διαδικτυακές τραπεζικές πύλες διασφαλίζονται με μοναδικά αναγνωριστικά στοιχεία χρήστη/πελάτη και κωδικούς πρόσβασης. Ορισμένες

	από αυτές χρειάζονται ένα ασφαλές κλειδί (συσκευή) που παράγει έναν μοναδικό κωδικό σε κάθε σύνδεση). **Πρόβλεψη απάτης** Στο πλαίσιο της ηλεκτρονικής τραπεζικής δραστηριότητας, η πρόβλεψη της απάτης επιτυγχάνεται με τη δημιουργία ενός προφίλ πελάτη με βάση ιστορικές πληροφορίες, που συλλέγονται κατά τη διάρκεια ηλεκτρονικών τραπεζικών δραστηριοτήτων (τερματικά που χρησιμοποιούνται, συνήθης χρόνος και τόπος σύνδεσης, διαδρομές σύνδεσης και δραστηριότητας κ.λπ.) και στη συνέχεια με την πρόβλεψη του βαθμού απάτης της τρέχουσας λειτουργίας, συγκρίνοντας την τρέχουσα συμπεριφορά του πελάτη με το προφίλ του. Εάν ο βαθμός απάτης θεωρείται υψηλός, η λειτουργία μπλοκάρεται. **Ανταπόκριση στην απάτη** Οι τράπεζες προσφέρουν επίσης απευθείας γραμμή (τηλεφωνική ή ηλεκτρονική) για την καταγγελία απάτης, καθώς και οδηγίες για την πρόληψη της απάτης. **Πρακτικές συμβουλές** • Χρησιμοποιείτε ασφαλείς κωδικούς πρόσβασης και αλλάζετε τους τακτικά • Επιλέξτε μοναδικούς κωδικούς πρόσβασης για κάθε ψηφιακό τραπεζικό λογαριασμό, μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για πολλούς λογαριασμούς. • Χρησιμοποιήστε ένα ασφαλές πρόγραμμα φύλαξης κωδικών πρόσβασης για την αποθήκευση των κωδικών σας • Αποφύγετε τη χρήση μη ασφαλούς δημόσιου Wi-Fi, όταν έχετε πρόσβαση σε οικονομικούς λογαριασμούς στο διαδίκτυο. • Μάθετε πώς να αναγνωρίζετε τις απάτες ηλεκτρονικού ταχυδρομείου ή κειμένου phishing • Επισκεφθείτε μόνο ασφαλείς ιστότοπους • Εγκαταστήστε προστασία κατά του spyware και του κακόβουλου λογισμικού στις συσκευές σας • Ρύθμιση ειδοποιήσεων για την παρακολούθηση των λογαριασμών σας και της δραστηριότητας συναλλαγών • Ενεργοποίηση ελέγχου ταυτότητας πολλαπλών παραγόντων

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**ONLINE ΠΛΗΡΩΜΕΣ**
Γενικές πληροφορίες	Οι ηλεκτρονικές πληρωμές γίνονται σε ιστοσελίδες ηλεκτρονικού εμπορίου μέσω πιστωτικών καρτών αλλά και μέσω ηλεκτρονικών πορτοφολιών. Οι τραπεζικές μεταφορές, οι εικονικές κάρτες και τα κουπόνια είναι επίσης άλλες μέθοδοι ψηφιακών πληρωμών. Σύμφωνα με την Statista, το 2019, ένας στους πέντε Ευρωπαίους προτίμησε να χρησιμοποιήσει εφαρμογές πληρωμών Fintech για τις διαδικτυακές αγορές του. Οι χρεωστικές κάρτες κατατάχθηκαν ως η πιο δημοφιλής μέθοδος ηλεκτρονικών πληρωμών, ενώ το Apple Pay και το Google Pay χρησιμοποιήθηκαν από περίπου το 3% των ερωτηθέντων. Όσον αφορά τα ηλεκτρονικά πορτοφόλια, τα στοιχεία δεν είναι ακόμη διαθέσιμα, αλλά πρόκειται για μια αγορά που αυξάνεται συνεχώς. Πλατφόρμες ηλεκτρονικών πληρωμών & ηλεκτρονικά πορτοφόλια: • PayPal • Google Pay • Apple Pay • Ali Pay • Samsung Pay • Mobikwik • Paytm • Amazon Pay • Πορτοφόλι Microsoft • Stipe • Klarna
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο: **Ιδιωτικότητα, ακρίβεια, ιδιοκτησία, προσβασιμότητα, παραβίαση νόμων, πνευματικά δικαιώματα**	Απόρρητο Εγκλήματα στον κυβερνοχώρο: κλοπή δεδομένων και ηλεκτρονική απάτη.
Εμπόδια/δυσκολίες για ενήλικες	Οι δυσκολίες που παρουσιάζονται για τους ηλικιακά μεγαλύτερους σχετίζονται με το θέμα του φόβου και της εμπιστοσύνης, καθώς οι περιπτώσεις απάτης στις πληρωμές είναι πολύ διαδεδομένες. Η άλλη δυσκολία αφορά την πρακτική χρήση αυτού του εργαλείου. Οι διάφοροι τύποι ηλεκτρονικών πληρωμών μπορεί να είναι δύσκολο να κατανοηθούν και τα πολυάριθμα βήματα που απαιτούνται για την ολοκλήρωσή τους μπορεί να είναι τεχνικά δύσκολα.

Κίνδυνος των μέσων κοινωνικής δικτύωσης /εργαλείων στους ενήλικες	**Απόρρητο** Ενώ σήμερα τα μετρητά επιτρέπουν ανώνυμες πληρωμές - και επομένως δεν υπάρχει εντοπισμός των αγορών που πραγματοποιούνται και δεν υπάρχει κίνδυνος για την ιδιωτική ζωή - δεν ισχύει το ίδιο για τις ηλεκτρονικές πληρωμές που είναι σε μεγάλο βαθμό ανιχνεύσιμες (διεύθυνση IP, όνομα, επώνυμο, διεύθυνση, αριθμός κάρτας κ.λπ.). **Κλοπή δεδομένων** Ο όγκος των δεδομένων που μοιράζονται κατά τις ηλεκτρονικές συναλλαγές πληρωμών εγείρει το ζήτημα της κλοπής δεδομένων. Σύμφωνα με την Έκθεση Norton Global Cyber Safety 2019, περισσότεροι από τους μισούς ερωτηθέντες είχαν βιώσει κάποιο έγκλημα στον κυβερνοχώρο, ενώ 1 στους 3 είχε πέσει θύμα τους τελευταίους 12 μήνες. 4,1 δισεκατομμύρια αρχεία εκτέθηκαν διεθνώς και υπήρξε αύξηση κατά 54% στον αριθμό των παραβιάσεων που αναφέρθηκαν. **Ηλεκτρονική απάτη** Σύμφωνα με την Ευρωπαϊκή Κεντρική Τράπεζα, η συνολική αξία των δόλιων συναλλαγών με χρήση καρτών που εκδόθηκαν παγκοσμίως ανήλθε σε 1,80 δισεκατομμύρια ευρώ το 2018. Όσον αφορά τις κάρτες που εκδίδονται μόνο στη ζώνη του ευρώ, η συνολική αξία των δόλιων συναλλαγών με κάρτες ανήλθε σε 0,94 δισ. ευρώ το 2018.
Λύσεις που μπορούμε να έχουμε	**Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) ή έλεγχος ταυτότητας δύο παραγόντων (2FA)** Πρόκειται για μια ηλεκτρονική μέθοδο πιστοποίησης ταυτότητας, κατά την οποία ένας χρήστης αποκτά πρόσβαση σε μια υπηρεσία μόνο μετά την επιτυχή παρουσίαση δύο ή περισσότερων αποδεικτικών στοιχείων (ή παραγόντων) σε έναν μηχανισμό πιστοποίησης ταυτότητας: **Γνώση**: κάτι που γνωρίζει μόνο ο χρήστης, συνήθως παρουσιάζεται ως απάντηση σε μια ερώτηση, όπως το όνομα ενός κατοικίδιου ζώου. **Κατοχή**: κάτι που έχει μόνο ο χρήστης, όπως ένα smartphone ή ένα κουπόνι. Στην περίπτωση του smartphone, θα σταλεί ένα sms στο τηλέφωνό σας με έναν κωδικό που πρέπει να πληκτρολογήσετε. **Εμπλοκή**: κάτι που αφορά μόνο τον χρήστη και περιλαμβάνει τη χρήση της αναγνώρισης ματιών και προσώπου ή δακτυλικών αποτυπωμάτων. **Ζητήστε το CVV** Είναι οι τρεις αριθμοί πίσω από την πιστωτική κάρτα και σας ζητείται κατά τη διάρκεια μιας ηλεκτρονικής συναλλαγής πληρωμής, για να βεβαιωθείτε ότι έχετε στην κατοχή σας την πιστωτική σας κάρτα. **Ασφαλής επεξεργασία πληρωμών**

	Πραγματοποιείται μέσω διαδικτυακών πυλών πληρωμών, οι οποίες είναι πιστοποιημένες κατά PCI, SSAE-16 και HIPAA. Οι πελάτες και οι πάροχοι δεν χρειάζεται να ανησυχούν για τη διαρροή και την κλοπή των ευαίσθητων δεδομένων τους από χάκερ.

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**INSTAGRAM**
Γενικές πληροφορίες	Το Instagram είναι μια αμερικανική υπηρεσία κοινωνικής δικτύωσης για κοινή χρήση φωτογραφιών και βίντεο. Η εφαρμογή επιτρέπει στους χρήστες να ανεβάζουν μέσα ενημέρωσης που μπορούν να επεξεργαστούν με φίλτρα και να οργανωθούν με hashtags και γεωγραφικές ετικέτες. Οι αναρτήσεις μπορούν να κοινοποιηθούν δημοσίως ή με προκαθορισμένους οπαδούς. Οι χρήστες μπορούν να περιηγηθούν στο περιεχόμενο άλλων χρηστών με βάση ετικέτες και τοποθεσίες και να δουν το περιεχόμενο που βρίσκεται σε τάση. Μπορούν να κάνουν like σε φωτογραφίες και να ακολουθούν άλλους χρήστες, για να προσθέσουν το περιεχόμενό τους σε μια προσωπική ροή. Η υπηρεσία πρόσθεσε επίσης λειτουργίες ανταλλαγής μηνυμάτων, τη δυνατότητα να συμπεριλάβετε πολλαπλές εικόνες ή βίντεο σε μία μόνο δημοσίευση και τη λειτουργία «Stories» που επιτρέπει στους χρήστες να δημοσιεύουν φωτογραφίες και βίντεο σε μια διαδοχική ροή, με κάθε δημοσίευση να είναι προσβάσιμη για 24 ώρες η κάθε μία. Στο τέλος του 2021, υπήρχαν 2,9 εκατομμύρια χρήστες στην Τσεχική Δημοκρατία. Πρόκειται για το ταχύτερα αναπτυσσόμενο δίκτυο. Είναι πιο δημοφιλές μεταξύ των χρηστών ηλικίας 15 έως 29 ετών.
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο: **Ιδιωτικότητα, ακρίβεια, ιδιοκτησία, προσβασιμότητα, παραβίαση νόμων, πνευματικά δικαιώματα**	Απόρρητο Κλοπή προφίλ Επίδραση στην ψυχική υγεία (καταθλιπτικά συμπτώματα, άγχος, στρες, εθισμός, ικανοποίηση από την εμφάνιση, ψευδής αυτο-παρουσίαση, εικόνα σώματος, μοναξιά, κοινωνικός αποκλεισμός, ικανοποίηση από τη ζωή κ.λπ.)
Εμπόδια/δυσκολίες για ενήλικες	Δυσκολία εύρεσης συνομηλίκων (το 71% των χρηστών του Instagram είναι κάτω των 35 ετών). Αίτημα για προσωπικά δεδομένα (όπως η ημερομηνία γέννησης). Ρυθμίσεις απορρήτου.
Κίνδυνος μέσου κοινωνικής	Απόρρητο - ο χρήστης του δικτύου θα πρέπει να προσέχει ποιον ακολουθεί και από ποιον ακολουθείται ή ποιος μπορεί να δει τις προσωπικές πληροφορίες και τις φωτογραφίες/βίντεο.

δικτύωσης/εργαλείων στους ενήλικες	Κλοπή προφίλ - ο λογαριασμός θα μπορούσε να «κλαπεί», οι φωτογραφίες του χρήστη θα μπορούσαν να χρησιμοποιηθούν κάπου αλλού ή οι χάκερ θα μπορούσαν να ενεργήσουν στο όνομά του.
Λύσεις που μπορούμε να έχουμε	Γνώση των εφαρμογών και των ρυθμίσεών τους, κανόνες συμπεριφοράς στο Instagram. Χρήση ισχυρού κωδικού πρόσβασης και τακτική αλλαγή του. Έλεγχος ταυτότητας δύο παραγόντων (σε υπολογιστή και στο τηλέφωνο). Ιδιωτικός λογαριασμός για προσωπικό προφίλ. Χρήση μόνο εξουσιοδοτημένων εφαρμογών.

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**SKYPE**
Γενικές πληροφορίες	Το Skype είναι μια ιδιόκτητη τηλεπικοινωνιακή εφαρμογή που λειτουργεί από την Skype Technologies, τμήμα της Microsoft, η οποία είναι περισσότερο γνωστή για τη βιντεοτηλεφωνία με βάση το VoIP, τις τηλεδιασκέψεις και τις φωνητικές κλήσεις. Διαθέτει επίσης άμεση ανταλλαγή μηνυμάτων, μεταφορά αρχείων, χρεωστικές κλήσεις προς σταθερά και κινητά τηλέφωνα (μέσω παραδοσιακών τηλεφωνικών δικτύων) και άλλες λειτουργίες. Το Skype είναι διαθέσιμο σε διάφορες πλατφόρμες επιτραπέζιων υπολογιστών, κινητών τηλεφώνων και κονσόλας βιντεοπαιχνιδιών. Η δημοτικότητα του skype αυξήθηκε σημαντικά κατά τη διάρκεια της πανδημίας.
Κίνδυνος που συνδέεται με τα μέσα κοινωνικής δικτύωσης/ εργαλείο: **Ιδιωτικότητα, ακρίβεια, ιδιοκτησία, προσβασιμότητα, παραβίαση νόμων, πνευματικά δικαιώματα**	Απόρρητο Κλοπή προφίλ Καταγραφή των κλήσεων (εγκλήματα στον κυβερνοχώρο)
Εμπόδια/δυσκολίες για ενήλικες	Ρυθμίσεις απορρήτου.
Κίνδυνος των μέσων κοινωνικής δικτύωσης/ εργαλείων στους ενήλικες	Ανεπιθύμητες κλήσεις. Δυσπιστία έναντι άλλων χρηστών.

Λύσεις που μπορούμε να έχουμε	Γνώση των εφαρμογών και των ρυθμίσεών τους. Καλά επιλεγμένο φόντο - προς τα πού δείχνει η κάμερα (για να μην φαίνεται ο εξοπλισμός του διαμερίσματος κ.λπ.). Απενεργοποιήστε τη φωτογραφική μηχανή, όταν δεν τη χρειάζεστε. Σιωπή κατά τη διάρκεια μιας κλήσης (μην ανοίγετε την τηλεόραση, για παράδειγμα), σίγαση του μικροφώνου όταν δεν είναι απαραίτητο. Χρήση ακουστικών. Να μην ανέχεστε την είσοδο ανεπιθύμητων συμμετεχόντων, να μην κάνετε κλικ σε ύποπτους συνδέσμους.

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**ΨΕΥΔΕΙΣ ΕΙΔΗΣΕΙΣ**
Γενικές πληροφορίες	Οι ψευδείς ειδήσεις, ή κοινώς παραπληροφόρηση, ορίζονται ως «ειδησεογραφικά άρθρα που είναι σκόπιμα και επαληθεύσιμα ψευδή και θα μπορούσαν να παραπλανήσουν τους αναγνώστες» (Allcott and Gentzkow, 2017, σ. 213. Ο όρος «ψευδείς ειδήσεις» δεν είναι καινούργιος. Οι Wardle και Derakhshan (2017) χώρισαν τον όρο fake news σε τρεις διαφορετικούς τύπους. Όρισαν την λανθασμένη πληροφόρηση ως «ψευδείς πληροφορίες που μοιράζονται χωρίς επιβλαβή πρόθεση», την εσκεμμένη παραπληροφόρηση ως «ψευδείς πληροφορίες που μοιράζονται με επιβλαβή πρόθεση» και, τέλος, την κακή πληροφόρηση ως «γνήσιες πληροφορίες που μοιράζονται για να προκαλέσουν βλάβη» (σελ. 5). Όπου αλλού, οι ερευνητές Lazer et al. (2018, σ. 2) όρισαν τις ψευδείς ειδήσεις ως «κατασκευασμένες πληροφορίες που μιμούνται το περιεχόμενο των ειδησεογραφικών μέσων ενημέρωσης ως προς τη μορφή, αλλά όχι ως προς την οργανωτική διαδικασία ή την πρόθεση». Ως εκ τούτου, ο όρος Fake-News αναφέρεται συχνά σε ειδήσεις που είναι ψευδείς, αλλά που εμφανίζονται ως νόμιμες ειδήσεις. Το διαδίκτυο είναι μια κοινή πηγή ψευδών ειδήσεων, με τις ψευδείς ειδήσεις να προωθούνται και να διαδίδονται συχνά στα μέσα κοινωνικής δικτύωσης. Οι ψευδείς ειδήσεις μπορεί να αφορούν οποιοδήποτε θέμα. Για παράδειγμα, έχει παραχθεί σημαντικός όγκος ψευδών ειδήσεων σχετικά με τον κορωνοϊό και τα εμβόλια.
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο:	Οι άνθρωποι σε όλο τον κόσμο γίνονται μάρτυρες μιας δραματικής αύξησης της πρόσβασης στην πληροφόρηση και την επικοινωνία. Ενώ κάποιοι

Ιδιωτικότητα, ακρίβεια, ιδιοκτησία, προσβασιμότητα, παραβίαση νόμων, πνευματικά δικαιώματα	λιμοκτονούν για πληροφορίες, άλλοι κατακλύζονται από έντυπο, ραδιοτηλεοπτικό και ψηφιακό περιεχόμενο. Πρόσφατες μελέτες που διεξήχθησαν παγκοσμίως μεταξύ των ανθρώπων έδειξαν ότι δυσκολεύονται να σκεφτούν κριτικά για τα μέσα ενημέρωσης και να κρίνουν την αξιοπιστία τους, ιδίως στο διαδίκτυο. Μεταξύ πολλών θεμάτων, η μελέτη έδειξε ότι οι περισσότεροι άνθρωποι δεν έχουν καλή κατανόηση του τι συνιστά τις «ψεύτικες ειδήσεις» έναντι των πραγματικών ειδήσεων: - δεν μπορούσαν να ξεχωρίσουν τα χορηγούμενα άρθρα από τις πραγματικές ειδήσεις - δεν μπήκαν στον κόπο να ελέγξουν από πού προέρχονται οι φωτογραφίες στο διαδίκτυο και αποδέχθηκαν τυφλά τα δηλωμένα συμφραζόμενα των φωτογραφιών. - δεν μπορούσαν να ξεχωρίσουν ένα πραγματικό ειδησεογραφικό άρθρο από ένα ψευδές ειδησεογραφικό άρθρο στα μέσα κοινωνικής δικτύωσης. - δεν μπορούσαν να αναγνωρίσουν το μεροληπτικό περιεχόμενο από ανεξάρτητες πηγές ειδήσεων που υποστηρίζονται από ομάδες όπως οι εταιρείες άσκησης πίεσης ως λιγότερο αξιόπιστο από μια κύρια πηγή ειδήσεων. Μπροστά στα πολλαπλά προβλήματα της ρητορικής του μίσους, του διαδικτυακού εκφοβισμού, του περιεχομένου του YouTube, των ψευδών ειδήσεων κ.λπ., παρατηρούμε επείγουσες εκκλήσεις για καλύτερη διαχείριση του περιβάλλοντος των μέσων ενημέρωσης - ιδίως για τη ρύθμιση του διαδικτύου. Όμως, μπροστά στις συγκρούσεις θετικών και αρνητικών δικαιωμάτων, στις ρυθμιστικές δυσκολίες, στις ισχυρές παγκόσμιες εταιρείες και στις βραχυπρόθεσμες πολιτικές σκοπιμότητες, η έκκληση αυτή με τη σειρά της μετατρέπεται γρήγορα σε έκκληση για την υποτιθέμενη «ηπιότερη» λύση της εκπαίδευσης του κοινού που χρησιμοποιεί το διαδίκτυο.
Εμπόδια/δυσκολίες για ενήλικες	Αυτό που ανησυχεί τους μελετητές είναι η επίδραση των ψευδών ειδήσεων στην αντίληψη του κοινού, που το αναγκάζει να λαμβάνει λογικές αποφάσεις με βάση την παραπληροφόρηση (Tandoc et al., 2018). Αυτό ισχύει ακόμη περισσότερο όταν οι χρήστες είναι πιο πιθανό να μοιραστούν αρνητικές ειδήσεις, και με την πρόσφατη πανδημία, υπάρχουν πολλές ειδήσεις που σχετίζονται με το Covid-19 και είναι αρνητικές (Nyilasy, n.d.). 374 Κατά συνέπεια, οι Chen κ.ά. (2011) τόνισαν την ανάγκη τα άτομα να είναι εγγράμματοι στα νέα μέσα ενημέρωσης, για να συμμετέχουν με επάρκεια σε αυτό το νέο περιβάλλον. Ο σημαντικότερος κίνδυνος που συνδέεται με τις «ψεύτικες ειδήσεις» είναι το γεγονός ότι απαξιώνει και απονομιμοποιεί τις φωνές εμπειρογνωμοσύνης, τους έγκυρους θεσμούς και την έννοια των αντικειμενικών δεδομένων - όλα

	αυτά υπονομεύουν την ικανότητα της κοινωνίας να συμμετέχει σε ορθολογικό διάλογο που βασίζεται σε κοινά γεγονότα. Επισημάνθηκαν τρεις συνακόλουθες βλάβες: πρώτον, το πρόβλημα του αυξανόμενου κατακερματισμού και της πολιτικοποίησης- δεύτερον, η προώθηση των «ασφαλών ειδήσεων» εις βάρος των δύσκολων ή προκλητικών ειδήσεων- τρίτον, η ανάγκη των αξιόπιστων πηγών να διαθέσουν ολοένα και λιγότερους πόρους για τη διάψευση ανακριβών πληροφοριών (που συνεπάγεται τόσο οικονομικό κόστος όσο και κόστος φήμης).
Κίνδυνος των μέσων κοινωνικής δικτύωσης /εργαλείων στους ενήλικες	Ο αυξανόμενος αριθμός των ηλικιακά μεγαλύτερων πολιτών που υιοθετούν ταχύτατα τα μέσα κοινωνικής δικτύωσης και γίνονται ευάλωτοι στην παραπληροφόρηση αποτελεί θέμα ιδιαίτερης ανησυχίας. Οι ηλικιακά μεγαλύτεροι χρήστες μπορεί να είναι ιδιαίτερα ευάλωτοι στα προβλήματα απορρόφησης ψευδών πληροφοριών, αλλά υπάρχουν παράγοντες που επηρεάζουν καθολικά όλες τις ηλικιακές ομάδες και την ικανότητα των ανθρώπων να διακρίνουν τα γεγονότα από τη φαντασία. Η ηλικία ενός ατόμου και η πηγή ενός περιεχομένου είναι σημαντικά κατά την ανάλυση της διάδοσης της παραπληροφόρησης, αλλά οι παράγοντες αυτοί δεν εξηγούν γιατί ορισμένοι άνθρωποι εξακολουθούν να πιστεύουν ψευδείς πληροφορίες πολύ καιρό μετά την παρουσίαση των στοιχείων που τις διορθώνουν. Ένας οργανισμός ελέγχου των γεγονότων δήλωσε ότι υπάρχουν τρεις παράγοντες που διαμορφώνουν την ικανότητα του καθενός να πέφτει θύμα ψευδών πληροφοριών. Ο πρώτος είναι η επανάληψη - αν μια λανθασμένη δήλωση επαναλαμβάνεται ξανά και ξανά, γίνεται πιο πιστευτή. Ο δεύτερος είναι ο τρόπος με τον οποίο εμφανίζεται η πληροφορία. Η έκθεση διαπίστωσε ότι το μέγεθος της γραμματοσειράς, η πολυπλοκότητα των λέξεων, η αντίθεση και η γραμματική επηρεάζουν το πόσο πιθανό είναι κάποιος να πιστέψει μια ψευδή δήλωση που κυκλοφορεί στο διαδίκτυο. Οι εικόνες τείνουν να γίνονται πιο εύκολα πιστευτές ως αληθινές, επειδή δημιουργούν την ψευδαίσθηση της πραγματικής απόδειξης ενός γεγονότος. Η έκθεση υπογραμμίζει επίσης την προκατάληψη που έχουν ήδη οι άνθρωποι πριν καταναλώσουν πληροφορίες. Οι απόψεις των ανθρώπων θα επηρεάσουν τον τρόπο με τον οποίο οι νέες πληροφορίες γίνονται αποδεκτές, ακόμη και όταν το άτομο γνωρίζει το αντίθετο. Οι πολιτικές ή κοινωνικές πεποιθήσεις μπορούν να εμποδίσουν τους ανθρώπους να δεχτούν πληροφορίες, παρά τα επίπεδα εκπαίδευσης ή την παιδεία τους στα μέσα ενημέρωσης. Οι περισσότεροι ηλικιακά μεγαλύτεροι έχουν ακούσει τον όρο fake news και γνωρίζουν ότι η παραπληροφόρηση στο διαδίκτυο αποτελεί πρόβλημα. Αν και άνθρωποι όλων των ηλικιών πέφτουν θύματα ψευδών ειδήσεων, μελέτες έχουν δείξει ότι οι ηλικιακά μεγαλύτεροι είναι πιο ευάλωτοι στις ψευδείς

	ειδήσεις και την ψηφιακή παραπληροφόρηση. Μια μελέτη έδειξε ότι οι χρήστες του Facebook ηλικίας 65 ετών και άνω δημοσίευσαν επτά φορές περισσότερα άρθρα από ιστότοπους με ψευδείς ειδήσεις από ό,τι οι ενήλικες ηλικίας 29 ετών και νεότεροι. Οι ηλικιακά μεγαλύτεροι ενήλικες είναι επίσης λιγότερο πιθανό να είναι σε θέση να εντοπίσουν τη διαφορά μεταξύ διαφημίσεων που έχουν σχεδιαστεί για να μοιάζουν με πραγματικές ειδήσεις και άρθρων που είναι πραγματικές ειδήσεις. Κλοπή προφίλ - ο λογαριασμός θα μπορούσε να "κλαπεί", οι φωτογραφίες του χρήστη θα μπορούσαν να χρησιμοποιηθούν κάπου αλλού ή οι χάκερ θα μπορούσαν να ενεργήσουν στο όνομά του.
Λύσεις που μπορούμε να έχουμε	Λόγω των παραπάνω προβλημάτων, μια εκτεταμένη έρευνα μεταξύ ηλικιωμένων πολιτών που διεξήχθη το 2009-2019 από τους Päivi Rasi, Hanna Vuojärvi και Susanna Rivinen αποκάλυψε ότι οι παρεμβάσεις θα πρέπει να προσφέρονται σε ηλικιωμένους με προβλήματα υγείας (Xie, 2011b), σε ηλικιωμένους άνω των 76 ετών, σε ηλικιωμένους με λιγότερη εμπειρία στην τεχνολογία και σε μειονοτικούς πληθυσμούς με χαμηλές δεξιότητες γραμματισμού στον τομέα της υγείας που ζουν σε διαφορετικές χώρες (Bertera, 2014- Lee & Kim, 2018- Vaportzis et al., 2017). Επίσης, θα πρέπει να παρέχονται παρεμβάσεις και υπηρεσίες και για τους ηλικιωμένους που βρίσκονται στο σπίτι και διατρέχουν μεγάλο κίνδυνο κοινωνικής απομόνωσης (Lee & Kim, 2018). Εκτός από την προσφορά κατάρτισης στη χρήση των ψηφιακών τεχνολογιών και μέσων (π.χ. González et al., 2015- Taha et al., 2016- Xie & Bugg, 2009), υπάρχει επίσης μεγάλη ανάγκη να αναπτυχθούν περισσότερες στρατηγικές για τη βελτίωση της αυτοπεποίθησης και της αυτό-αποτελεσματικότητας των ηλικιακά μεγαλύτερων στις διαδικτυακές δραστηριότητες (Chu & Chu, 2010). Οι παρεμβάσεις θα πρέπει να στοχεύουν στον γραμματισμό των ηλικιακά μεγαλύτερων στα μέσα ενημέρωσης και στην ηλεκτρονική υγεία (Manafò & Wong, 2013- Xie, 2012- Young et al., 2012). Οι πρακτικές συνέπειες της ενασχόλησης με τις ικανότητες των ηλικιακά μεγαλύτερων να δημιουργούν περιεχόμενο στα μέσα ενημέρωσης, ιδίως η ανάγκη να δοθεί προσοχή στην ικανότητα των ηλικιακά μεγαλύτερων να αφηγούνται προσωπικές και δημόσιες ιστορίες για τη ζωή τους, ώστε να αμφισβητείται η κυρίαρχη αναπαράσταση της δημογραφικής τους ομάδας, τονίζονται ιδιαίτερα (Manchester & Facer, 2015). Ο Νόμος της Ευρωπαϊκής Επιτροπής για τις Ψηφιακές Υπηρεσίες προτίθεται να αντιμετωπίσει και να καταστήσει την επιφάνεια των παρόχων ασφαλέστερη. Ωστόσο, κάθε πολίτης πρέπει να κάνει ό,τι μπορεί για να αναπτύξει τις κατάλληλες δεξιότητες, ώστε να προστατεύσει τον εαυτό του από βλάβες. Ο Thierri Breton, Επίτροπος για την Εσωτερική Αγορά, δήλωσε: «Πρέπει να τιθασεύσουμε την πανδημία πληροφόρησης (infodemic) και τη διάδοση ψευδών πληροφοριών που θέτουν σε κίνδυνο τη ζωή των ανθρώπων. Η παραπληροφόρηση δεν μπορεί να παραμείνει πηγή εσόδων. Πρέπει να δούμε ισχυρότερες δεσμεύσεις από τις διαδικτυακές πλατφόρμες, ολόκληρο το

	διαφημιστικό οικοσύστημα και τα δίκτυα ελέγχου των γεγονότων. Ο Νόμος για τις Ψηφιακές Υπηρεσίες θα μας παράσχει πρόσθετα, ισχυρά εργαλεία για την αντιμετώπιση της παραπληροφόρησης». «Ο ψηφιακός γραμματισμός είναι μια δεξιότητα που μπορεί να διδαχθεί και να αναπτυχθεί.» Έχει γίνει πιο σημαντικό για τους ηλικιωμένους να μάθουν να διακρίνουν την παραπληροφόρηση από τις πραγματικές ειδήσεις. Αν πιστέψετε το επιχείρημα ότι οι ηλικιακά μεγαλύτεροι δυσκολεύονται περισσότερο να εντοπίσουν τις ψευδείς ειδήσεις από ό,τι οι νεότερες ομάδες λόγω ψηφιακού αναλφαβητισμού, τότε προκύπτει ότι αυτό είναι ένα πρόβλημα που μπορεί να αντιμετωπιστεί μέσω της ψηφιακής εκπαίδευσης. Ο ψηφιακός γραμματισμός είναι κάτι που μπορεί να διδαχθεί και να βελτιωθεί. Ένας τρόπος είναι να παρακολουθήσετε ένα μάθημα ή ένα διαδικτυακό σεμινάριο για τον ψηφιακό γραμματισμό. Αυτά τα μαθήματα διδάσκουν στους ηλικιωμένους πώς να ελέγχουν τα γεγονότα και παρέχουν εργαλεία και τεχνικές για την αξιολόγηση του διαδικτυακού περιεχομένου. **Ποια μέτρα μπορούν να λάβουν οι ηλικιακά μεγαλύτεροι για να αποφύγουν να πέσουν θύματα ψευδών ειδήσεων;** Ένας ηλικιωμένος πολίτης ισχυρίστηκε ότι «τώρα συνειδητοποιώ ότι οι ψευδείς ειδήσεις είναι πολύ πιο περίπλοκες και ύπουλες από ό,τι νόμιζα.» Οι ψευδείς ειδήσεις δεν είναι καινούργιες, ωστόσο- από τότε που οι λέξεις μπορούσαν να ειπωθούν ή να γραφτούν στο χαρτί, η παραπληροφόρηση υπήρχε είτε σκόπιμα είτε λανθασμένα. Όπως το έθεσε ένα άρθρο του Guardian: «Η εποχή της μετα-αλήθειας, πράγματι, εκτείνεται όσο πίσω θέλετε να κοιτάξετε, δεν υπήρξε ποτέ μια χρυσή εποχή διαφάνειας.» Είτε η έννοια των ψευδών ειδήσεων είναι καινούργια είτε όχι, η κατανάλωση πληροφοριών ειδικά τώρα απαιτεί μια εργαλειοθήκη δεξιοτήτων. Μπορεί να είναι ιδιαίτερα χρήσιμη η χρήση μιας σειράς ερωτήσεων που θα βοηθήσουν στην αξιολόγηση των νέων πληροφοριών. Όταν προσπαθείτε να προσδιορίσετε αν κάτι είναι αληθινό, ρωτήστε τον εαυτό σας: Ποιος έγραψε τις πληροφορίες; Τι προσόντα έχει ο συντάκτης του άρθρου; Είναι οι πληροφορίες ενημερωμένες; Είναι ο ιστότοπος αξιόπιστος; Προσπαθούν να σας πουλήσουν κάποιο προϊόν; Χορηγεί κάποια εταιρεία ή οργανισμός τον ιστότοπο; Υποστηρίζει ο δικτυακός τόπος εναλλακτικές ή διαφορετικές απόψεις για το θέμα που συζητείται;

	Άλλες πρακτικές στρατηγικές **Ελέγξτε την πηγή και το πλαίσιο** Οι ιστοσελίδες είναι αξιόπιστες ή έμπιστες πηγές; «Η παραπληροφόρηση μπορεί να προέρχεται από πολλά μέρη - δεν αρκεί να αποφεύγετε εκεί που νομίζετε ότι θα είναι. Είναι καλύτερο να έχετε ένα φίλτρο από το οποίο περνούν όλες οι πληροφορίες.» Ελέγξτε, για παράδειγμα, πώς τελειώνει μια ιστοσελίδα. Αν τελειώνει με .gov ή .edu είναι επίσημη κυβερνητική ιστοσελίδα ή εκπαιδευτικό ίδρυμα, αντίστοιχα. Το Senior Planet δίνει επίσης έμφαση στην κατανόηση του πλαισίου, όπως η αναγνώριση της σάτιρας. Είναι εύκολο να μπερδέψετε μια αστεία εικόνα ή ένα αστείο άρθρο ως αληθινό. **Να είστε παρατηρητικοί και στην εικόνα** Αναζητήστε ασύνδετες γωνίες ή/και περίεργο φωτισμό, για να εντοπίσετε αν οι εικόνες έχουν παραποιηθεί. Και πάλι, σημειώστε την πηγή και το πλαίσιο. **Γνώμες έναντι γεγονότων** Κατανοήστε τη διάκριση μεταξύ γνώμης και γεγονότων, ιδίως επειδή ο καθένας μπορεί να δημοσιεύσει περιεχόμενο στο διαδίκτυο. Η «παράπλευρη ανάγνωση» - ή ο έλεγχος άλλων αξιόπιστων πηγών για την επαλήθευση πληροφοριών κατά την ανάγνωση - είναι ένας όρος που χρησιμοποιήθηκε για πρώτη φορά από την Ομάδα Εκπαίδευσης Ιστορίας του Στάνφορντ. Βασικές ερωτήσεις που πρέπει να κάνετε στον εαυτό σας καθώς το κάνετε αυτό: «Ποιος κρύβεται πίσω από την πληροφορία; Ποια είναι τα αποδεικτικά στοιχεία; Τι λένε άλλες πηγές;» Οι βιβλιοθήκες μπορούν επίσης να παρέχουν χρήσιμες πηγές. Οι βιβλιοθήκες μπορεί να προσφέρουν εκδηλώσεις για να μάθετε για την παιδεία στα μέσα ενημέρωσης - και οι βιβλιοθηκονόμοι είναι εκπαιδευμένοι να «αναλύουν τις πληροφορίες και όλο τον θόρυβο κάθε μέρα». Κάντε παύση πριν κοινοποιήσετε ή αντιδράσετε στο διαδίκτυο. «Κάντε παύση, σκεφτείτε και συγκρατηθείτε». Το να κάνετε κάποιον να ασχοληθεί περισσότερο με click – bait περιεχόμενο μέσω likes ή σχολίων μπορεί να είναι ένας τρόπος για τους ιστότοπους να παράγουν έσοδα. Εάν φίλοι ή συγγενείς κοινοποιούν παραπληροφόρηση στο διαδίκτυο, προσφέρετε τους πηγές ελέγχου των γεγονότων. Προσοχή σε bots και trolls Τα bots είναι ψεύτικοι αυτοματοποιημένοι λογαριασμοί. Αναγνωρίστε τους εντοπίζοντας νέους λογαριασμούς με λίγους followers, χωρίς φωτογραφία, περίεργα ονόματα χρηστών με πολλούς αριθμούς και μη λογικά ή εμπρηστικά σχόλια. Τα bots και τα trolls είναι συχνά ταραχοποιοί στο διαδίκτυο. Είτε πρόκειται για bots είτε όχι, σκεφτείτε δύο φορές αν θέλετε να εμπλακείτε στο διαδίκτυο με κάποιον που δεν γνωρίζετε. Είναι απαραίτητο ή εποικοδομητικό να το κάνετε;

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**ΑΠΑΤΕΣ ΜΕΣΩ EMAIL**
Γενικές πληροφορίες	Το ηλεκτρονικό ταχυδρομείο είναι ένας από τους πιο ωφέλιμους τρόπους επικοινωνίας. Είναι επίσης ένα βασικό εργαλείο που χρησιμοποιείται από επιτιθέμενους για την κλοπή χρημάτων, στοιχείων λογαριασμών και ευαίσθητων πληροφοριών. Εάν οι χρήστες αλληλεπιδρούν με τον απατεώνα ηλεκτρονικού ταχυδρομείου και παρέχουν ευαίσθητες πληροφορίες, αυτό μπορεί να προκαλέσει μακροπρόθεσμα προβλήματα, όπως κλοπή ταυτότητας, οικονομική απώλεια και καταστροφή δεδομένων. Η απάτη μέσω ηλεκτρονικού ταχυδρομείου είναι εσκεμμένη εξαπάτηση είτε για προσωπικό όφελος, είτε για να ζημιωθεί ένα άλλο άτομο μέσω ηλεκτρονικού ταχυδρομείου. Σχεδόν αμέσως μόλις το ηλεκτρονικό ταχυδρομείο έγινε ευρέως γνωστό, άρχισε να χρησιμοποιείται για την εξαπάτηση ανθρώπων. Η απάτη μέσω ηλεκτρονικού ταχυδρομείου μπορεί να λάβει τη μορφή ενός «παιχνιδιού απάτης» ή απάτης. Τα κόλπα εμπιστοσύνης τείνουν να εκμεταλλεύονται την εγγενή απληστία και ανεντιμότητα των θυμάτων τους. Η προοπτική μιας «ευκαιρίας» ή ενός «κάτι για το τίποτα» μπορεί να είναι πολύ δελεαστική. Η απάτη μέσω ηλεκτρονικού ταχυδρομείου, όπως και άλλες «απάτες bunco», στοχεύει συνήθως σε αφελή άτομα που εμπιστεύονται τα σχέδιά τους για γρήγορο πλουτισμό. Αυτά περιλαμβάνουν «πολύ καλές για να είναι αληθινές» επενδύσεις ή προσφορές για την πώληση δημοφιλών αντικειμένων σε «απίστευτα χαμηλές» τιμές. Πολλοί άνθρωποι έχουν χάσει τις οικονομίες τους λόγω απάτης.
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο: **Ιδιωτικότητα, ακρίβεια, ιδιοκτησία, προσβασιμότητα, παραβίαση νόμων, πνευματικά δικαιώματα**	Πολλές απάτες μέσω ηλεκτρονικού ταχυδρομείου υπάρχουν εδώ και πολύ καιρό. Στην πραγματικότητα, αρκετές από αυτές είναι απλώς «ανακυκλωμένες» απάτες που προϋπήρχαν της χρήσης του ηλεκτρονικού ταχυδρομείου. **Απάτες LOTTERY** Λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που ισχυρίζεται ότι κερδίσατε μια άγνωστη λοταρία, και πάντα με ένα τεράστιο κέρδος. Μπορεί επίσης να σας ζητηθεί να πληρώσετε ένα μικρό ποσό για να «απελευθερώσετε» τα κέρδη σας. Σας ζητείται να στείλετε προσωπικά στοιχεία ως επαλήθευση και ξαφνικά γίνεστε θύμα απάτης ταυτότητας και τα χρήματα που στείλατε έχουν χαθεί. **Προσφορές εργασίας και ψεύτικες επιχειρηματικές ευκαιρίες** Αυτές οι απάτες υπόσχονται την ευκαιρία να κερδίσετε πολλά χρήματα με πολύ λίγη προσπάθεια. Συνήθως είναι γεμάτες με δελεαστικά λόγια όπως «Εργαστείτε μόνο μερικές ώρες την εβδομάδα», «Γίνετε αφεντικό του εαυτού

	σας», «Ορίστε το δικό σας ωράριο» και «Εργαστείτε από το σπίτι». Τα μηνύματα ηλεκτρονικού ταχυδρομείου που προσφέρουν αυτές τις «ευκαιρίες» έχουν συχνά γραμμές θέματος που μοιάζουν με τις ακόλουθες: «Κερδίστε ένα τακτικό εισόδημα Online», «Βάλτε τον υπολογιστή σας να δουλέψει για εσάς!»: eBay Insider Secrets Revealed 6228; Get Rich Click Λαμβάνετε ένα ανεπιθύμητο μήνυμα ηλεκτρονικού ταχυδρομείου που σας προσφέρει μια θέση εργασίας, συνήθως όχι στον τομέα της εξειδίκευσής σας, συχνά για μια θέση μυστικού αγοραστή ή παρόμοια θέση. Όταν αποδέχεστε, πληρώνεστε με επιταγή ή έμβασμα, για ποσό μεγαλύτερο από αυτό που προσέφερε ο «εργοδότης» σας. Στη συνέχεια, σας ζητείται να στείλετε πίσω τη διαφορά, μόνο και μόνο για να ανακαλύψετε ότι η αρχική επιταγή ή το αρχικό χρηματικό ένταλμα ήταν πλαστό, και ότι δεν έχετε τα χρήματα που στείλατε στον ψεύτικο εργοδότη σας. Στις περισσότερες περιπτώσεις, το μήνυμα ηλεκτρονικού ταχυδρομείου παρέχει πολύ λίγες λεπτομέρειες σχετικά με τη φύση της επιχειρηματικής ευκαιρίας. Τα περισσότερα παρέχουν μια διεύθυνση ή έναν ιστότοπο από τον οποίο μπορείτε, έναντι αμοιβής, να λάβετε ένα «πακέτο πληροφοριών» σχετικά με την ευκαιρία. Αυτές οι ευκαιρίες, ωστόσο, συνήθως δεν είναι τίποτε άλλο από συστήματα πυραμίδας στα οποία η «ευκαιρία» περιλαμβάνει την ικανότητά σας να στρατολογήσετε περισσότερους ανυποψίαστους ανθρώπους για να αγοράσουν την απάτη. Τελικά, η απάτη αποκαλύπτεται ή η δεξαμενή νέων προσλήψεων στερεύει και αποτυγχάνει. **Φιλανθρωπικές απάτες** Μετά από φυσικές καταστροφές μεγάλης κλίμακας ή δημόσιες τραγωδίες υψηλού προφίλ, οι απατεώνες προσπαθούν να επωφεληθούν από το δημόσιο συναίσθημα. Δημιουργούν ψεύτικους ιστότοπους και λογαριασμούς δωρεών και ένα συναισθηματικό μήνυμα ηλεκτρονικού ταχυδρομείου, για να ζητήσουν χρήματα που δεν φτάνουν ποτέ στα θύματα. Αυτές οι απάτες μπορεί να είναι επιτυχείς, επειδή παίζουν με την καλή θέληση των ανθρώπων! **Απάτες δικαιούχων** Λαμβάνετε ένα email από κάποιον που θέλει να διακινήσει γρήγορα κάποια χρήματα. Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου προέρχονται μερικές φορές από ανθρώπους που ισχυρίζονται ότι είναι ένας σημαντικός επιχειρηματίας ή λειτουργός, ο οποίος λέει ότι έχει εκατομμύρια να μεταφέρει εκτός της χώρας και θέλει τη βοήθειά σας με αντάλλαγμα ένα μερίδιο από τα κέρδη. **Μιμητής** Πολλές απάτες μιμούνται νόμιμες εταιρείες σε μια προσπάθεια να ξεγελάσουν τους καταναλωτές. Ο απλούστερος τρόπος για να αποφύγετε αυτές τις απομιμήσεις είναι να μην κάνετε ποτέ κλικ σε έναν σύνδεσμο που αποστέλλεται

	σε ένα ανεπιθύμητο μήνυμα ηλεκτρονικού ταχυδρομείου. Βρείτε μόνοι σας τον σύνδεσμο της εταιρείας, χρησιμοποιώντας μια μηχανή αναζήτησης ή, αν γνωρίζετε τη διεύθυνση της εταιρείας, πληκτρολογήστε την μόνοι σας. **Απάτες επισκευής PC** Μια απάτη που ξεκινάει στον πραγματικό κόσμο και γρήγορα μεταφέρεται στον διαδικτυακό. Λαμβάνετε ένα τηλεφώνημα από κάποιον που ισχυρίζεται ότι εργάζεται για τη «Microsoft» ή άλλη μεγάλη εταιρεία λογισμικού και ισχυρίζεται ότι μπορεί να επιλύσει προβλήματα του υπολογιστή σας, όπως οι αργές ταχύτητες του Διαδικτύου. Ακούγεται χρήσιμο, και έτσι, όταν το email φτάνει στα εισερχόμενά σας, κατεβάζετε ένα πρόγραμμα απομακρυσμένης πρόσβασης, το οποίο επιτρέπει στους απατεώνες να πάρουν τον έλεγχο του υπολογιστή σας. **«Επίσημη ανακοίνωση»** Αυτές οι απάτες προσπαθούν να ξεγελάσουν τους καταναλωτές και να τους κάνουν να πιστέψουν ότι έλαβαν ένα μήνυμα ηλεκτρονικού ταχυδρομείου που απαιτεί από αυτούς να προβούν σε κάποια ενέργεια. Συχνά υποτίθεται ότι προέρχονται από κυβερνητικές υπηρεσίες και σας ενημερώνουν για κάποιο πρόβλημα. Αυτό το παράδειγμα εστάλη τον Μάιο, μια εποχή κατά την οποία οι άνθρωποι είναι πιο πιθανό να πιστέψουν ότι μια ανακοίνωση προέρχεται από την IRS. Εδώ υποτίθεται ότι πρέπει να ανακουφιστείτε που η IRS αναγνωρίζει ότι έλαβε την πληρωμή σας και στη συνέχεια να αγχωθείτε ότι υπάρχει πρόβλημα και να κάνετε κλικ χωρίς να το σκεφτείτε. **Έρευνα** Αυτές οι απάτες βασίζονται στην επιθυμία των ανθρώπων να τοποθετηθούν επί των θεμάτων. Σε μια χρονιά εκλογών, μπορεί να σας σταλεί μια έρευνα για την ψήφο σας ή για οποιοδήποτε άλλο επίκαιρο θέμα: η υπερθέρμανση του πλανήτη, η στάση απέναντι στον πόλεμο, η αντιμετώπιση της τελευταίας φυσικής καταστροφής και ούτω καθεξής. **Απάτες που βασίζονται στην υγεία και διατροφή** Αυτές οι απάτες εκμεταλλεύονται τις ανασφάλειες που έχουν ορισμένοι άνθρωποι σχετικά με την κατάσταση της ευεξίας τους. Επειδή μπορεί να διστάζουν ή να ντρέπονται να συζητήσουν τα προβλήματά τους με έναν γιατρό ή δεν έχουν την οικονομική δυνατότητα να αγοράσουν νόμιμα φάρμακα ή θεραπεία, δελεάζονται με υποσχέσεις για γρήγορες λύσεις και εκπληκτικά αποτελέσματα, εκπτωτικές τιμές, γρήγορη παράδοση, απαλλαγή από συνταγογράφηση, προστασία της ιδιωτικής ζωής και διακριτική συσκευασία. Τέτοια ηλεκτρονικά μηνύματα έχουν γραμμές θέματος που μοιάζουν με τις ακόλουθες: Αυξήστε δραστικά τη σεξουαλική σας απόδοση- ΕΛΕΓΧΕΤΕ ΤΟ ΒΑΡΟΣ ΣΑΣ!!!- Χρειάζεται να χάσετε βάρος για το καλοκαίρι;- Φυσικό φάρμακο υγείας που λειτουργεί!- Μειώστε το σωματικό λίπος και χτίστε άπαχους μυς

	χωρίς άσκηση- Νέοι σε κάθε ηλικία- Απομακρύνετε χρόνια από την εμφάνισή σας- Δίνει ενέργεια και καίει λίπος. **Trojan Horse Email (Ιός ηλεκτρονικού υπολογιστή)** Τα μηνύματα ηλεκτρονικού ταχυδρομείου αυτού του τύπου προσφέρουν την υπόσχεση για κάτι που μπορεί να σας ενδιαφέρει - ένα συνημμένο αρχείο που περιέχει ένα αστείο, μια φωτογραφία ή μια επιδιόρθωση για μια ευπάθεια λογισμικού. Ωστόσο, όταν ανοίξει, το συνημμένο μπορεί να κάνει κάποιο ή όλα τα ακόλουθα: να δημιουργήσει μια ευπάθεια ασφαλείας στον υπολογιστή σας- να ανοίξει μια μυστική «κερκόπορτα» για να επιτρέψει σε έναν εισβολέα μελλοντική παράνομη πρόσβαση στον υπολογιστή σας- να εγκαταστήσει λογισμικό που καταγράφει τις πληκτρολογήσεις σας και στέλνει τα αρχεία καταγραφής σε έναν εισβολέα, επιτρέποντας στον εισβολέα να βρει τους κωδικούς πρόσβασης και άλλες σημαντικές πληροφορίες- να εγκαταστήσει λογισμικό που παρακολουθεί τις συναλλαγές και τις δραστηριότητές σας στο διαδίκτυο- να παρέχει σε έναν εισβολέα πρόσβαση στα αρχεία σας- να μετατρέψει τον υπολογιστή σας σε ένα «ρομπότ» που μπορεί να χρησιμοποιήσει ο εισβολέας για να στείλει ανεπιθύμητα μηνύματα, να εξαπολύσει επιθέσεις άρνησης παροχής υπηρεσιών ή να εξαπλώσει τον ιό σε άλλους υπολογιστές. Μηνύματα τέτοιου τύπου έχουν έρθει σε διάφορες συσκευασίες κατά τη διάρκεια των ετών. Ένας από τους πιο γνωστούς ιούς ήταν ο ιός "Love Bug", ο οποίος μεταφερόταν με ένα μήνυμα ηλεκτρονικού ταχυδρομείου με θέμα "I Love You" και ζητούσε από τον παραλήπτη να δει το συνημμένο "ερωτικό γράμμα". Άλλα μηνύματα τέτοιου τύπου παριστάνουν μια εικονική καρτ-ποστάλ, ή ένα email από προμηθευτή λογισμικού, που ζητά από τον παραλήπτη να εφαρμόσει ένα συνημμένο "patch", ή ένα email με τη γραμμή θέματος "funny" που ενθαρρύνει τον παραλήπτη να δει το συνημμένο "αστείο" ή ένα email που ισχυρίζεται ότι προέρχεται από έναν προμηθευτή antivirus και ενθαρρύνει τον παραλήπτη να εγκαταστήσει δωρεάν το συνημμένο "virus sweeper". **Ηλεκτρονικό ταχυδρομείο που δημιουργείται από ιό** Σημειώστε ότι, σε ορισμένες περιπτώσεις, μια γνωστή διεύθυνση "από" δεν εξασφαλίζει την ασφάλεια: Πολλοί ιοί εξαπλώνονται αναζητώντας πρώτα όλες τις διευθύνσεις ηλεκτρονικού ταχυδρομείου σε έναν μολυσμένο υπολογιστή και στη συνέχεια στέλνοντας σε αυτές τις διευθύνσεις. Έτσι, αν ο υπολογιστής ενός φίλου σας έχει μολυνθεί από έναν τέτοιο ιό, μπορεί να λάβετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που μπορεί να προέρχεται πράγματι από τον υπολογιστή του φίλου σας, αλλά το οποίο στην πραγματικότητα δεν έχει συνταχθεί από τον φίλο σας. Αν έχετε αμφιβολίες, επαληθεύστε το μήνυμα με το άτομο που πιστεύετε ότι είναι ο αποστολέας πριν ανοίξετε οποιοδήποτε συνημμένο email.

	Παρακαλούμε βρείτε έναν εκτενή κατάλογο των διαφόρων τύπων απάτης ηλεκτρονικού ταχυδρομείου στον σύνδεσμο https://en.wikipedia.org/wiki/Email_fraud
Εμπόδια/δυσκολίες για ενήλικες	Όπως και σε κάθε άλλο είδος απάτης, ο δράστης μπορεί να προκαλέσει σημαντική ζημιά, ιδίως όταν η απειλή επιμένει για μεγάλο χρονικό διάστημα. Η απάτη μέσω ηλεκτρονικού ταχυδρομείου έχει έναν κατάλογο αρνητικών επιπτώσεων , συμπεριλαμβανομένης της απώλειας χρημάτων, της απώλειας πνευματικής ιδιοκτησίας, της ζημιάς στη φήμη, μερικές φορές με ανεπανόρθωτες επιπτώσεις. Αν και οι ηλικιακά μεγαλύτεροι σπάνια αναφέρουν ότι πέφτουν θύματα οικονομικού ηλεκτρονικού εγκλήματος, υπάρχουν στοιχεία που δείχνουν ότι οι ηλικιακά μεγαλύτεροι χρήστες του διαδικτύου διατρέχουν αυξημένο κίνδυνο. Μια εμπεριστατωμένη έρευνα διερεύνησε πώς, γιατί και υπό ποιες συνθήκες οι ενήλικες μεγαλύτερης ηλικίας γίνονται θύματα ηλεκτρονικού εγκλήματος και εξέτασε ορθολογικές στρατηγικές παρέμβασης. Σύμφωνα με την έρευνα, η κοινωνική απομόνωση, τα γνωστικά, σωματικά και ψυχικά προβλήματα υγείας- η περιουσιακή κατάσταση, οι περιορισμένες δεξιότητες ή η ευαισθητοποίηση στον τομέα της ασφάλειας στον κυβερνοχώρο, οι κοινωνικές συμπεριφορές και το περιεχόμενο των απατών οδήγησαν στη θυματοποίηση. Διαπίστωσε ότι μέχρι σήμερα έχουν δοκιμαστεί οι περισσότερες παρεμβάσεις για την ενίσχυση της ευαισθητοποίησης και των δεξιοτήτων των ηλικιακά μεγαλύτερων χρηστών του διαδικτύου. Άλλες θεωρητικά εύλογες παρεμβάσεις περιλαμβάνουν: προγράμματα διαχείρισης παραβατών, προσαρμοσμένα μέτρα ασφαλείας, μείωση του στίγματος σε ολόκληρη την κοινωνία και ευαισθητοποίηση ομάδων που υποστηρίζουν ηλικιωμένους.
Κίνδυνος μέσων κοινωνικής δικτύωσης/εργαλείων στους ενήλικες	Η εξαπάτηση των ηλικιακά μεγαλύτερων είναι ένα τεράστιο πρόβλημα σε όλο τον κόσμο. Οι απάτες που ξεκινούν από το Διαδίκτυο γίνονται όλο και πιο συχνές και σε αυτόν τον πληθυσμό, ιδίως καθώς οι ηλικιακά μεγαλύτεροι που γνωρίζουν το Διαδίκτυο αρχίζουν να γερνούν. Οι απατεώνες δεν κάνουν διακρίσεις όσον αφορά το από ποιον προσπαθούν να αποσπάσουν χρήματα: πλούσιους, φτωχούς, μαύρους, λευκούς, 65 ετών και υγιείς, 85 ετών και ασθενείς. Θα προσπαθήσουν να πάρουν χρήματα από οποιονδήποτε. Η έρευνα εκτιμά ότι περίπου το 5% του ηλικιωμένου πληθυσμού (που αντιστοιχεί σε περίπου δύο έως τρία εκατομμύρια άτομα) υποφέρει από κάποιο είδος απάτης κάθε χρόνο. «Το χειρότερο είναι ότι είναι πολύ πιθανό να πρόκειται για υποεκτίμηση». Αυτό είναι πολύ πιθανό επειδή αναμένεται ότι ένα μεγάλο ποσοστό απάτης μέσω του Διαδικτύου δεν καταγγέλλεται. Η εξαπάτηση των ηλικιακά μεγαλύτερων είναι μια γιγαντιαία επιχείρηση που αφαιρεί από τους ηλικιωμένους τα συνταξιοδοτικά τους κεφάλαια και τις

	κρατικές παροχές. Επισημαίνει ότι οι ηλικιακά μεγαλύτεροι χάνουν περίπου 3 δισεκατομμύρια δολάρια από τους απατεώνες κάθε χρόνο. Λιγότερο συντηρητικές εκτιμήσεις αναφέρουν ότι οι ηλικιακά μεγαλύτεροι χάνουν έως και 36 δισεκατομμύρια δολάρια κάθε χρόνο. Αναφέρεται επίσης ότι το μέσο ποσό που έχασε κάποιος άνω των 80 ετών ήταν πάνω από 1.000 δολάρια και το μέσο ποσό που έχασε κάποιος μεταξύ 70 και 79 ετών ήταν πάνω από 600 δολάρια. **Γιατί οι ηλικιακά μεγαλύτεροι πέφτουν θύματα απάτης μέσω ηλεκτρονικού ταχυδρομείου; Τα κύρια ζητήματα** Πάρα πολλοί ηλικιωμένοι πέφτουν θύματα απάτης, αλλά δεν φταίνε οι ίδιοι. Αυτός ο πληθυσμός είναι σε μεγάλο βαθμό αξιόπιστος και αποτελείται από οικονομικά γόνιμους ανθρώπους των οποίων η γνωστική ικανότητα μπορεί να έχει μειωθεί λόγω διαφόρων παθήσεων. Ας ερευνήσουμε τα χαρακτηριστικά και τους λόγους για τους οποίους οι ηλικιακά μεγαλύτεροι γίνονται ευάλωτοι στους απατεώνες. Εκτός από το γιατί οι ηλικιακά μεγαλύτεροι μπορεί να γίνουν στόχος, οι απάτες αυτές έχουν διάφορες μορφές που εκμεταλλεύονται τα τρωτά σημεία τους. **Απομόνωση** Η μοναξιά μπορεί να καταστρέψει πολλές πτυχές της ζωής ενός ηλικιωμένου, μεταξύ άλλων καθιστώντας τον εξαιρετικά ευάλωτο σε απάτες. Κατ' αρχάς, όταν είναι απομονωμένοι, δεν υπάρχει κανείς που να τους ελέγχει τα οικονομικά τους. Μπορεί να είναι πολύ αργά για να κάνετε κάτι, αν ένα αγαπημένο πρόσωπο το ανακαλύψει μετά από χρόνια. Οι απομονωμένοι ηλικιακά μεγαλύτεροι μπορεί επίσης να είναι πιο ευάλωτοι στην κοινωνική αλληλεπίδραση, γεγονός που μπορεί να τους προετοιμάσει για έναν πρόθυμο απατεώνα που χρησιμοποιεί μια «σχέση» για να ξεκινήσει το σχέδιό του. **Οικονομική κατάσταση** Η οικονομική κατάσταση των ηλικιακά μεγαλύτερων είναι ένας σημαντικός λόγος για τον οποίο γίνονται στόχοι για απάτες. Από τη μία πλευρά, ένας ηλικιωμένος μπορεί να έχει εκατομμύρια δολάρια στη διάθεσή του μετά την αποταμίευση για τη συνταξιοδότηση και τη λήψη μηνιαίων επιταγών σύνταξης και κρατικών παροχών. Αυτό μπορεί να κάνει το άτομο λιγότερο αυστηρό με τα χρήματά του, γεγονός που με τη σειρά του καθιστά ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή ένα μήνυμα από έναν «εγγονό» που ζητά χρήματα μια εύκολη υπόθεση. Από την άλλη πλευρά, ένας ηλικιωμένος θα μπορούσε να είναι οικονομικά ανασφαλής και να έχει ανάγκη από μια πηγή εισοδήματος για γρήγορο πλουτισμό, καθιστώντας ένα σύστημα πυραμίδας ελκυστικό, χωρίς να γνωρίζει ότι δεν θα πάρει ποτέ πίσω τα χρήματά του.

	Εμπιστοσύνη Σύμφωνα με έρευνες, οι άνθρωποι που μεγάλωσαν στις δεκαετίες του 1920, του '30 και του '40, δηλαδή εκείνοι που γίνονται συχνά στόχος απάτης, είναι γενικά πιο έμπιστοι από άλλες γενιές, γεγονός που τους καθιστά ευάλωτους στους απατεώνες. **Ανασφάλεια** Μερικές φορές, οι ηλικιακά μεγαλύτεροι απλώς εκφοβίζονται και αναγκάζονται να παραδώσουν χρήματα σε απατεώνες. Είτε αυτοπροσώπως είτε μέσω τηλεφώνου, ένας απατεώνας μπορεί να πιέσει ανελέητα έναν ηλικιωμένο για χρήματα μέχρι να σπάσει. Επιπλέον, ένας απατεώνας μπορεί να στοχεύσει στις ανασφάλειες ενός ηλικιωμένου ατόμου, όπως η υγεία του ή η κοινωνική του θέση, λέγοντας ότι πρέπει να πληρώσει έναν συγκεκριμένο ιατρικό λογαριασμό, αλλιώς δεν θα μπορεί πλέον να λαμβάνει κρατική ασφάλιση υγείας. **Μειωμένη γνώση** Καθώς γερνάμε, είναι πιο πιθανό να εμφανίσουμε κάποιο είδος γνωστικής πάθησης του εγκεφάλου, όπως η άνοια, η οποία επηρεάζει τη μνήμη και τη συνολική γνωστική λειτουργία. Αυτές οι γνωστικές παθήσεις μπορούν να επηρεάσουν τη μνήμη σας με μύριους τρόπους, όπως το ποια είναι η οικογένειά σας και πόσα χρήματα έχετε - και τι είναι αληθινό ή ψεύτικο. Οι απατεώνες θα επιτεθούν σε αυτές τις αδυναμίες. Για παράδειγμα, ένας απατεώνας μπορεί να καλέσει κάποιον 80άρη προσποιούμενος ότι είναι το εγγόνι του. Ο ηλικιωμένος μπορεί να θυμάται ότι έχει εγγόνι, αλλά μπορεί να μην θυμάται τα πραγματικά τους ονόματα ή πώς ακούγονται, οπότε θα συμφωνήσει με ό,τι λέει ο απατεώνας. **Αμηχανία** Οι ηλικιακά μεγαλύτεροι μπορεί απλώς να ντρέπονται να αναφέρουν στις αρχές ότι είναι θύματα απάτης. Αυτό τους καθιστά ελκυστικούς στόχους, επειδή οι απατεώνες γνωρίζουν ότι υπάρχει μεγάλη πιθανότητα να μην τους πιάσουν. Συν τοις άλλοις, πολλοί ηλικιωμένοι δεν έχουν ιδέα πού να καταγγείλουν τις απάτες, πράγμα που δυστυχώς είναι ακόμη καλύτερο για τους απατεώνες. Λιγότερο συντηρητικές εκτιμήσεις αναφέρουν ότι οι ηλικιακά μεγαλύτεροι χάνουν έως και 36 δισεκατομμύρια δολάρια κάθε χρόνο. Αναφέρεται επίσης ότι το μέσο ποσό που έχασε κάποιος άνω των 80 ετών ήταν πάνω από 1.000 δολάρια και το μέσο ποσό που έχασε κάποιος μεταξύ 70 και 79 ετών ήταν πάνω από 600 δολάρια.
Λύσεις που μπορούμε να έχουμε	Το ηλεκτρονικό ταχυδρομείο είναι ένα βολικό και ισχυρό εργαλείο επικοινωνίας. Δυστυχώς, παρέχει και στους απατεώνες και σε άλλα κακόβουλα άτομα ένα εύκολο μέσο, για να προσελκύσουν πιθανά θύματα. Οι απάτες που επιχειρούν κυμαίνονται από τις κλασσικές επιχειρήσεις bait –and- switch μέχρι τα συστήματα ηλεκτρονικού «ψαρέματος» που χρησιμοποιούν έναν συνδυασμό ηλεκτρονικού ταχυδρομείου και ψεύτικων ιστότοπων για να

	εξαπατήσουν τα θύματα, ώστε να αποκαλύψουν ευαίσθητες πληροφορίες. Για να προστατευτείτε από αυτές τις απάτες, θα πρέπει να καταλάβετε τι είναι, πώς μοιάζουν, πώς λειτουργούν και τι μπορείτε να κάνετε για να τις αποφύγετε. Οι παρακάτω βασικές συστάσεις μπορούν να ελαχιστοποιήσουν τις πιθανότητες να πέσετε θύμα απάτης μέσω ηλεκτρονικού ταχυδρομείου: Φίλτρο ανεπιθύμητης αλληλογραφίας. Μην εμπιστεύεστε ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου. Αντιμετωπίστε τα συνημμένα αρχεία με προσοχή. Μην κάνετε κλικ σε συνδέσμους σε μηνύματα ηλεκτρονικού ταχυδρομείου. Εγκαταστήστε λογισμικό προστασίας από ιούς και διατηρήστε το ενημερωμένο. Εγκαταστήστε ένα προσωπικό τείχος προστασίας και διατηρήστε το ενημερωμένο. Ρυθμίστε το πρόγραμμα-πελάτη ηλεκτρονικού ταχυδρομείου σας για ασφάλεια. **Τι μπορείτε να κάνετε για να μη γίνετε θύμα;** **Φίλτρο για Spam** Επειδή οι περισσότερες απάτες ηλεκτρονικού ταχυδρομείου ξεκινούν με ανεπιθύμητα εμπορικά μηνύματα, θα πρέπει να λάβετε μέτρα για να αποτρέψετε την είσοδο ανεπιθύμητων μηνυμάτων στα εισερχόμενά σας. Οι περισσότερες εφαρμογές ηλεκτρονικού ταχυδρομείου και οι υπηρεσίες διαδικτυακής αλληλογραφίας περιλαμβάνουν λειτουργίες φιλτραρίσματος ανεπιθύμητης αλληλογραφίας ή τρόπους με τους οποίους μπορείτε να ρυθμίσετε τις εφαρμογές ηλεκτρονικού ταχυδρομείου σας, ώστε να φιλτράρουν την ανεπιθύμητη αλληλογραφία. Συμβουλευτείτε το αρχείο βοήθειας της εφαρμογής ή της υπηρεσίας ηλεκτρονικού ταχυδρομείου σας για να μάθετε τι πρέπει να κάνετε για να φιλτράρετε τα ανεπιθύμητα μηνύματα. Μπορεί να μην μπορείτε να διαγράψετε όλα τα ανεπιθύμητα μηνύματα, αλλά το φιλτράρισμα θα αποτρέψει μεγάλο μέρος τους από το να φτάσουν στα εισερχόμενά σας. Θα πρέπει να γνωρίζετε ότι οι spammers παρακολουθούν τα εργαλεία και το λογισμικό φιλτραρίσματος spam και λαμβάνουν μέτρα για να τα αποφύγουν. Για παράδειγμα, οι spammers μπορεί να χρησιμοποιούν διακριτικά ορθογραφικά λάθη, για να παρακάμψουν τα φίλτρα spam, αλλάζοντας το "Potency Pills" σε "Potençy Pills". **Να είστε καχύποπτοι απέναντι στα ανεπιθύμητα emails** Μην εμπιστεύεστε αυτόματα οποιοδήποτε μήνυμα ηλεκτρονικού ταχυδρομείου σας αποστέλλεται από άγνωστο άτομο ή οργανισμό. Ποτέ μην ανοίγετε συνημμένα αρχεία σε ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου. Το πιο σημαντικό, μην κάνετε ποτέ κλικ σε σύνδεσμο που σας αποστέλλεται σε ηλεκτρονικό ταχυδρομείο. Οι έξυπνα κατασκευασμένοι σύνδεσμοι μπορεί να σας οδηγήσουν σε πλαστογραφημένους ιστότοπους που

	έχουν δημιουργηθεί, για να σας εξαπατήσουν ώστε να αποκαλύψετε προσωπικές πληροφορίες ή να κατεβάσετε ιούς, spyware και άλλο κακόβουλο λογισμικό. Οι spammers μπορεί επίσης να χρησιμοποιούν μια τεχνική κατά την οποία στέλνουν μοναδικούς συνδέσμους σε κάθε μεμονωμένο μήνυμα spam. Το θύμα 1 μπορεί να λάβει ένα μήνυμα ηλεκτρονικού ταχυδρομείου με τον σύνδεσμο <http://dfnasdunf.example.org/> και το θύμα 2 μπορεί να λάβει το ίδιο μήνυμα spam με τον σύνδεσμο <http://vnbnnasd.exaple.org/>. Παρακολουθώντας ποιοι σύνδεσμοι ζητούνται στους διακομιστές ιστού τους, οι spammers μπορούν να καταλάβουν ποιες διευθύνσεις ηλεκτρονικού ταχυδρομείου είναι έγκυρες και να στοχεύουν με μεγαλύτερη ακρίβεια τα θύματα για επαναλαμβανόμενες προσπάθειες spam. Να θυμάστε ότι ακόμη και το email που αποστέλλεται από μια οικεία διεύθυνση μπορεί να δημιουργήσει προβλήματα: Πολλοί ιοί εξαπλώνονται ανιχνεύοντας τον υπολογιστή-θύμα για διευθύνσεις ηλεκτρονικού ταχυδρομείου και αποστέλλονται σε αυτές τις διευθύνσεις με το πρόσχημα ενός μηνύματος ηλεκτρονικού ταχυδρομείου από τον ιδιοκτήτη του μολυσμένου υπολογιστή. **Αντιμετωπίστε τα συνημμένα email με προσοχή** Τα συνημμένα αρχεία ηλεκτρονικού ταχυδρομείου χρησιμοποιούνται συνήθως από επιτήδειους για να περάσουν κρυφά έναν ιό στον υπολογιστή σας. Αυτοί οι ιοί μπορούν να βοηθήσουν τον απατεώνα να κλέψει σημαντικές πληροφορίες από τον υπολογιστή σας, να θέσει σε κίνδυνο τον υπολογιστή σας ώστε να είναι ανοιχτός σε περαιτέρω επιθέσεις και καταχρήσεις και να μετατρέψει τον υπολογιστή σας σε «ρομπότ» για χρήση σε επιθέσεις άρνησης παροχής υπηρεσιών και άλλα διαδικτυακά εγκλήματα. Όπως προαναφέρθηκε, μια γνωστή διεύθυνση αποστολέα δεν αποτελεί εγγύηση ασφάλειας, επειδή ορισμένοι ιοί εξαπλώνονται αναζητώντας πρώτα όλες τις διευθύνσεις ηλεκτρονικού ταχυδρομείου σε έναν μολυσμένο υπολογιστή και στη συνέχεια στέλνοντας σε αυτές τις διευθύνσεις. Μπορεί ο υπολογιστής του φίλου σας να έχει μολυνθεί από έναν τέτοιο ιό. **Χρησιμοποιήστε την κοινή λογική** Όταν φτάνει στα εισερχόμενά σας ένα μήνυμα ηλεκτρονικού ταχυδρομείου που σας υπόσχεται πολλά χρήματα για λίγη προσπάθεια, σας κατηγορεί για παραβίαση του Patriot Act ή σας προσκαλεί να συμμετάσχετε σε μια συνωμοσία για την αρπαγή αζήτητων χρημάτων με τη συμμετοχή αγνώστων προσώπων σε μια χώρα στην άλλη άκρη του κόσμου, σκεφτείτε μια στιγμή την πιθανότητα το μήνυμα να είναι νόμιμο. **Εγκαταστήστε λογισμικό Antivirus και διατηρήστε το ενημερωμένο** Εάν δεν το έχετε κάνει μέχρι τώρα, θα πρέπει να εγκαταστήσετε λογισμικό προστασίας από ιούς στον υπολογιστή σας. Εάν είναι δυνατόν, θα πρέπει να εγκαταστήσετε ένα πρόγραμμα προστασίας από ιούς που διαθέτει λειτουργία

	αυτόματης ενημέρωσης. Αυτό θα σας βοηθήσει να διασφαλίσετε ότι έχετε πάντα την πιο ενημερωμένη δυνατή προστασία από τους ιούς. Επιπλέον, θα πρέπει να βεβαιωθείτε ότι το λογισμικό προστασίας από ιούς που επιλέγετε περιλαμβάνει λειτουργία σάρωσης ηλεκτρονικού ταχυδρομείου. Αυτό θα σας βοηθήσει να διατηρήσετε τον υπολογιστή σας απαλλαγμένο από ιούς που μεταδίδονται μέσω ηλεκτρονικού ταχυδρομείου. **Εγκαταστήστε ένα πρόγραμμα προστασίας και διατηρήστε το ενημερωμένο** Ένα πρόγραμμα προστασίας δεν θα αποτρέψει την εισροή μηνυμάτων ηλεκτρονικού ταχυδρομείου απάτης στα εισερχόμενά σας. Ωστόσο, μπορεί να σας βοηθήσει να προστατευτείτε σε περίπτωση που ανοίξετε κατά λάθος ένα συνημμένο αρχείο που περιέχει ιό ή εισαγάγετε με άλλο τρόπο κακόβουλο λογισμικό στον υπολογιστή σας, ακολουθώντας τις οδηγίες του ηλεκτρονικού ταχυδρομείου. Το πρόγραμμα προστασίας, μεταξύ άλλων, θα βοηθήσει στην αποτροπή της εξερχόμενης κυκλοφορίας από τον υπολογιστή σας προς τον επιτιθέμενο. Όταν το προσωπικό σας πρόγραμμα προστασίας ανιχνεύει ύποπτες εξερχόμενες επικοινωνίες από τον υπολογιστή σας, αυτό μπορεί να αποτελεί ένδειξη ότι έχετε εγκαταστήσει κατά λάθος κακόβουλα προγράμματα στον υπολογιστή σας. **Μάθετε τις πολιτικές ηλεκτρονικού ταχυδρομείου των οργανισμών με τους οποίους συνεργάζεστε** Οι περισσότεροι οργανισμοί που δραστηριοποιούνται διαδικτυακά έχουν πλέον σαφείς πολιτικές σχετικά με τον τρόπο επικοινωνίας με τους πελάτες τους μέσω ηλεκτρονικού ταχυδρομείου. Πολλοί, για παράδειγμα, δεν θα σας ζητήσουν να δώσετε πληροφορίες λογαριασμού ή προσωπικές πληροφορίες μέσω ηλεκτρονικού ταχυδρομείου. Η κατανόηση των πολιτικών των οργανισμών με τους οποίους συνεργάζεστε μπορεί να σας βοηθήσει να εντοπίσετε και να αποφύγετε το phishing και άλλες απάτες. Σημειώστε, ωστόσο, ότι δεν είναι ποτέ καλή ιδέα να στέλνετε ευαίσθητες πληροφορίες μέσω μη κρυπτογραφημένου ηλεκτρονικού ταχυδρομείου. **Διαμόρφωση του ηλεκτρονικού ταχυδρομείου σας για ασφάλεια** Υπάρχουν διάφοροι τρόποι με τους οποίους μπορείτε να ρυθμίσετε το email σας, ώστε να είστε λιγότερο ευάλωτοι σε απάτες μέσω ηλεκτρονικού ταχυδρομείου. Για παράδειγμα, η ρύθμιση των παραμέτρων του προγράμματος ηλεκτρονικού ταχυδρομείου σας, ώστε να προβάλλεται το ηλεκτρονικό ταχυδρομείο ως «μόνο κείμενο» θα σας βοηθήσει να προστατευτείτε από απάτες που χρησιμοποιούν καταχρηστικά το HTML στο ηλεκτρονικό ταχυδρομείο. **Άλλοι τρόποι προστασίας από απάτες μέσω ηλεκτρονικού ταχυδρομείου** Η πρόληψη, μέσω της ευαισθητοποίησης, αποτελεί ζωτικό εργαλείο για την καταπολέμηση των απατεώνων. Υπάρχουν ορισμένες χρήσιμες συμβουλές που

	θα σας βοηθήσουν να αποφύγετε την απάτη στο τηλέφωνο, στο διαδίκτυο, μέσω ταχυδρομείου ή στο σπίτι σας. Υπάρχουν μερικές γενικές συμβουλές, για να προστατευτείτε από το να πέσετε θύμα απάτης. Ποτέ μην δίνετε προσωπικές πληροφορίες. Μπορούν να χρησιμοποιηθούν για την κλοπή της ταυτότητάς σας και την πρόσβαση σε λογαριασμούς. Ελέγχετε πάντα τα εύσημα οποιασδήποτε εταιρείας ή νομικού επαγγελματία για τον οποίο δεν είστε σίγουροι. Μπορείτε να τους αναζητήσετε στο Companies House (εξωτερικός σύνδεσμος ανοίγει σε νέο παράθυρο/καρτέλα) για να μάθετε το ιστορικό τους ή να αναζητήσετε κριτικές στο διαδίκτυο. Μην δίνετε προκαταβολές μέχρι να βεβαιωθείτε ότι η εταιρεία με την οποία συναλλάσσεστε είναι νόμιμη. Αποφύγετε την προσθήκη σε λίστες αλληλογραφίας, τις οποίες μερικές φορές παίρνουν στα χέρια τους οι απατεώνες. **Ενδείξεις για να εντοπίσετε emails απάτης** Οι απατεώνες γίνονται όλο και πιο επιδέξιοι στην παραποίηση μηνυμάτων ηλεκτρονικού ταχυδρομείου και πλαστών μηνυμάτων, σε διάφορες γλώσσες. Είναι πάντα σημαντικό να αναζητάτε τα σημάδια μιας πλαστογραφίας, όπως : Γενικοί χαιρετισμοί Κακή ποιότητα γραμματικής, λεξιλογίου Πιθανά ορθογραφικά λάθη Ατελής σχεδιασμός γραφικών στοιχείων **Κάντε αυτές τις ερωτήσεις** Γιατί με προσεγγίζουν; Είναι αυτό πολύ καλό ή πολύ κακό για να είναι αληθινό; Ξέρω πραγματικά ποιος είναι ο διαδικτυακός μου έρωτας; Συνάντησα ποτέ τον διαδικτυακό μου έρωτα; Είχα ποτέ τηλεφωνική ή βιντεοσκοπημένη σύνδεση μαζί του; Μου ζητάει επανειλημμένα χρήματα, επικαλούμενος πιθανά έξοδα ταξιδιού, αγορές διαβατηρίων ή διάφορα δραματικά πράγματα και άλλες ιστορίες; **SCAM TEST - Χρησιμοποιήστε αυτά τα βήματα για να σαρώσετε τα email σας** Φαίνεται πολύ καλό για να είναι αληθινό Επικοινώνησε ξαφνικά Ζητήθηκαν προσωπικά στοιχεία

	Ζητούνται χρήματα ΘΥΜΗΘΕΙΤΕ: χρηματοπιστωτικά ιδρύματα, εταιρείες κοινής ωφέλειας, αρχές επιβολής του νόμου, κυβερνητικοί φορείς, πάροχοι διαδικτύου και τηλεπικοινωνιών ή άλλοι δημόσιοι φορείς: Δεν θα σας ζητήσει ΠΟΤΕ την πληρωμή σε κουπόνια. Δεν θα σας ζητήσει ΠΟΤΕ να μεταφέρετε χρήματα, επειδή ο λογαριασμός σας έχει παραβιαστεί. ΠΟΤΕ δεν θα σας απειλήσει στο τηλέφωνο, με επιστολή ή ηλεκτρονικό ταχυδρομείο για τη μη καταβολή μιας αμοιβής. ΠΟΤΕ δεν θα απειλήσει με σύλληψη εάν η πληρωμή δεν γίνει αμέσως. ΠΟΤΕ δεν θα ζητήσετε χρήματα για «δωρεάν δώρο», «αμοιβή διαχείρισης» ή ως μέρος μιας προώθησης. ΠΟΤΕ δεν θα σας ζητήσει να αποκαλύψετε τους κωδικούς ασφαλείας του λογαριασμού σας ή τους διαδικτυακούς κωδικούς πρόσβασης στο σύνολό τους. ΠΟΤΕ δεν θα καλέσει ξαφνικά και δεν θα ζητήσει απομακρυσμένη πρόσβαση στον υπολογιστή ή τις συσκευές σας ή να κατεβάσει λογισμικό. Δεν θα σας ενημερώσει ΠΟΤΕ για τις φορολογικές δηλώσεις μέσω ηλεκτρονικού ταχυδρομείου, κειμένου ή φωνητικού μηνύματος.

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**PHISHING (Ηλεκτρονικό ψάρεμα)**
Γενικές πληροφορίες	Οι απάτες με στόχο τους ηλικιωμένους είναι μια πολύ μεγάλη επιχείρηση που κλέβει από τις αποταμιεύσεις, τα συνταξιοδοτικά κεφάλαια, ακόμη και τα κρατικά επιδόματα των ηλικιωμένων. Οι ζημιές μπορεί να είναι καταστροφικές. Πέραν από τις πολλές μεθόδους που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου για να εξαπατήσουν τους ηλικιωμένους, το phishing είναι μία από τις παλαιότερες και πιο γνωστές. Το phishing είναι ένα είδος διαδικτυακής απάτης κατά την οποία οι απατεώνες χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο και άλλες μεθόδους, για να κλέψουν προσωπικές πληροφορίες, όπως οικονομικά στοιχεία ή κωδικούς πρόσβασης λογαριασμών. Το όνομα της προσέγγισης αυτής οφείλεται στο γεγονός ότι χρησιμοποιεί ελκυστικά «δολώματα», για να παρασύρει τους ανθρώπους σε ιστότοπους και να ζητήσει τα δεδομένα τους με ψευδείς προφάσεις. Το phishing δεν είναι το ίδιο με το spam. Το spam είναι απλώς ένας άλλος όρος για την ανεπιθύμητη αλληλογραφία και τις ανεπιθύμητες διαφημίσεις, οι επιθέσεις phishing είναι σκόπιμες προσπάθειες να κλέψουν τις πληροφορίες σας και να τις χρησιμοποιήσουν με επιβλαβείς τρόπους. Οι απάτες ηλεκτρονικού ταχυδρομείου Phishing πραγματοποιούνται διαδικτυακά από τεχνίτες με τεχνολογικές γνώσεις και εγκληματίες που διαπράττουν κλοπές ταυτότητας. Χρησιμοποιούν ανεπιθύμητα μηνύματα, ψεύτικους ιστότοπους που

	έχουν κατασκευαστεί, ώστε να μοιάζουν πανομοιότυποι με πραγματικούς ιστότοπους, ηλεκτρονικά μηνύματα και άμεσα μηνύματα, για να σας εξαπατήσουν, ώστε να αποκαλύψετε ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης τραπεζικών λογαριασμών και αριθμούς πιστωτικών καρτών. Μόλις τσιμπήσετε το δόλωμα του phisher, μπορεί να χρησιμοποιήσει τις πληροφορίες για να δημιουργήσει ψεύτικους λογαριασμούς στο όνομά σας, να καταστρέψει την πιστοληπτική σας ικανότητα και να κλέψει τα χρήματά σας ή ακόμη και την ταυτότητά σας.
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο: **Ιδιωτικότητα, ακρίβεια, ιδιοκτησία, προσβασιμότητα, παραβίαση νόμων, πνευματικά δικαιώματα**	Μια απάτη ηλεκτρονικού ψαρέματος αποτελείται από τρία βασικά στοιχεία: (1) Η επίθεση πραγματοποιείται μέσω ηλεκτρονικών επικοινωνιών. Αν και το ηλεκτρονικό ταχυδρομείο είναι συνηθισμένο, το phishing μπορεί επίσης να πραγματοποιηθεί μέσω μηνυμάτων κειμένου, λογαριασμών στα μέσα κοινωνικής δικτύωσης, φωνητικού ταχυδρομείου, ακόμη και τηλεφωνικών κλήσεων. (2) Όλες οι μορφές phishing έχουν ως στόχο να σας πείσουν ότι μια ψεύτικη επικοινωνία είναι πραγματική και αξιόπιστη. Ο επιτιθέμενος ισχυρίζεται ότι είναι ένα άτομο ή ένας οργανισμός που σας είναι οικείος και αξιόπιστος. (3) Στόχος μιας επίθεσης phishing είναι η απόκτηση ευαίσθητων προσωπικών πληροφοριών, όπως στοιχεία σύνδεσης, τραπεζικά στοιχεία ή αριθμούς πιστωτικών καρτών. Σε όλες τις επιθέσεις phishing, ο απατεώνας παραδίδει ένα προσεκτικά σχεδιασμένο μήνυμα με στόχο να σας παρακινήσει να κάνετε κλικ σε έναν σύνδεσμο, να κατεβάσετε ένα συνημμένο αρχείο ή να δώσετε συγκεκριμένες προσωπικές πληροφορίες. Μερικά κοινά παραδείγματα επιθέσεων phishing περιλαμβάνουν: **Έκκληση για βοήθεια:** Ο επιτιθέμενος, με στόχο να σας τραβήξει το ενδιαφέρον, σας στέλνει ένα email προσποιούμενος έναν καλό φίλο ή συγγενή (π.χ. το εγγόνι σας). Ισχυρίζεται ότι βρίσκεται σε οικονομική δυσπραγία και ζητά τη βοήθειά σας άμεσα. Πώς είναι σε θέση οι εγκληματίες του κυβερνοχώρου να υποδύονται ανθρώπους που γνωρίζετε; Με τα μέσα κοινωνικής δικτύωσης, οι απατεώνες έχουν πρόσβαση σε περισσότερες προσωπικές μας πληροφορίες από ποτέ. Αυτό τους επιτρέπει να κάνουν τα μηνύματά τους εξαιρετικά στοχευμένα -και συχνά πολύ πιστευτά. **Είσαι ο μεγάλος νικητής:** Πρόκειται για ένα ακαταμάχητο ταξιδιωτικό πακέτο ή για δωρεάν εισιτήρια για μια εκδήλωση. Σας ζητείται να δώσετε τα προσωπικά σας στοιχεία προκειμένου να διεκδικήσετε το βραβείο σας. **Ο τραπεζικός σας λογαριασμός έχει παραβιαστεί:** Λαμβάνετε μια «επείγουσα» ειδοποίηση που φαίνεται να προέρχεται από την τράπεζά σας, η οποία σας προειδοποιεί για ύποπτη δραστηριότητα στο λογαριασμό σας. Στη συνέχεια, σας ζητείται να κάνετε κλικ σε έναν σύνδεσμο που σας μεταφέρει σε έναν ιστότοπο, όπου σας ζητείται να επιβεβαιώσετε τα στοιχεία του τραπεζικού σας λογαριασμού.

	Η κυβέρνηση σας κυνηγάει: Λίγα πράγματα στη ζωή είναι τόσο ενοχλητικά όσο μια έγκυρη ειδοποίηση από έναν κυβερνητικό οργανισμό. Οι απατεώνες το γνωρίζουν αυτό, γι' αυτό και πολλά μηνύματα ηλεκτρονικού «ψαρέματος» εμφανίζονται ως κυβερνητικά. Ένα τέτοιο μήνυμα ηλεκτρονικού ταχυδρομείου έχει συνήθως απειλητικό τόνο και αναφέρει μεγάλες, τρομακτικές ποινές - εκτός αν παρέχετε την πληρωμή ή τα προσωπικά δεδομένα που ζητούν. Αυτού του είδους οι επιθέσεις phishing έχουν και μια άλλη πλευρά. Σε ορισμένες περιπτώσεις, αποστέλλονται κατά τη διάρκεια της φορολογικής περιόδου, προσφέροντάς σας μια γενναιόδωρη επιστροφή χρημάτων, αφού επιβεβαιώσετε τα οικονομικά σας στοιχεία. **Γιατί το phishing λειτουργεί τόσο καλά;** Τα μηνύματα ηλεκτρονικού ταχυδρομείου, τα μηνύματα κειμένου, τα μηνύματα φωνητικού ταχυδρομείου, ακόμη και οι φωνητικές κλήσεις δεν πιστοποιούνται. Αυτό σημαίνει ότι, όπως ακριβώς και μια καρτ ποστάλ που αποστέλλεται μέσω ταχυδρομείου, δεν υπάρχει κανένας πραγματικός τρόπος να επικυρωθεί από πού προήλθαν. Αυτό δίνει στους απατεώνες μεγάλη ελευθερία να μιμούνται αξιόπιστες μάρκες στις επικοινωνίες τους. Το phishing είναι μία από τις πιο κοινές και διαδεδομένες απειλές. Οι εξελιγμένοι phishers είναι πολύ επιδέξιοι στο να δημιουργούν ψεύτικα πρότυπα email και ιστότοπους που δεν ξεχωρίζουν από τους πραγματικούς, μέχρι και τη διεύθυνση URL (διεύθυνση ιστότοπου) και τα πιστοποιητικά ασφαλείας. Μπορεί να νομίζετε ότι λαμβάνετε ένα αξιόπιστο μήνυμα από μια τράπεζα, ένα ηλεκτρονικό κατάστημα ή μια εταιρεία πιστωτικών καρτών. Και αν δεν δίνετε μεγάλη προσοχή, μπορεί να μην αντιληφθείτε την απάτη πριν να είναι αργά. **Τύποι Phishing που πρέπει να γνωρίζετε για να παραμείνετε ασφαλείς** Το «ψάρεμα» πραγματοποιείται συνήθως μέσω παραποίησης ηλεκτρονικού ταχυδρομείου, άμεσων μηνυμάτων και μηνυμάτων κειμένου. Πρόκειται για έναν παραπλανητικό τρόπο που κάνει τα άτομα να αποκαλύψουν προσωπικές πληροφορίες. Είναι επίσης μια μορφή εξαπάτησης για τη λήψη κακόβουλου λογισμικού ή ransomware σε ένα σύστημα. Με οποιονδήποτε τρόπο, ο δράστης αποκτά προνομιακή πρόσβαση σε ευαίσθητες πληροφορίες. Πρόκειται για μια ολοένα και πιο σοβαρή απειλή, επειδή υπάρχουν πολλοί τρόποι μέσω των οποίων οι δράστες επιτίθενται. Το «ψάρεμα» έχει εξελιχθεί σε ό,τι χρειάζονται οι εγκληματίες του κυβερνοχώρου, για να κλέψουν τα προσωπικά στοιχεία σας. Οι μέθοδοί τους λαμβάνουν πλέον πολλές μορφές. Αν δεν είστε εξοικειωμένοι με όρους όπως smishing, vishing, pharming και BEC, ακολουθεί ένας οδηγός: **ΤΥΠΙΚΟ PHISHING** Απλώνω παντού τα δίχτυά μου- Στην πιο βασική του μορφή, το τυπικό phishing είναι η απόπειρα κλοπής εμπιστευτικών πληροφοριών με τους απατεώνες να προσποιούνται ότι είναι ένα εξουσιοδοτημένο άτομο ή οργανισμός. Δεν είναι στοχευμένη επίθεση και μπορεί να διεξαχθεί μαζικά.

EMAIL PHISHING

Το πιο συνηθισμένο σενάριο phishing έχει τη μορφή κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου που αποστέλλονται σε άτομα και μιμούνται έναν αυθεντικό οργανισμό. Γνωστό και ως spam phishing, αυτό το είδος επίθεσης επιτρέπει στον εγκληματία του κυβερνοχώρου να αποκτήσει πρόσβαση σε μεγάλο αριθμό πελατών που είναι εγγεγραμμένοι σε έναν ιστότοπο. Έτσι, τα μηνύματα ηλεκτρονικού ταχυδρομείου phishing αποστέλλονται συχνά μαζικά. Υπάρχει μεγάλη πιθανότητα επιτυχίας, αφού συχνά κάποια άτομα από το πλήθος θα πέσουν θύματα.

ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ PHISHING

Χρησιμοποιώντας τις ίδιες τεχνικές, αυτός ο τύπος phishing εισάγει κακούς ιούς, πείθοντας τον χρήστη να κάνει κλικ σε έναν σύνδεσμο ή να κατεβάσει ένα συνημμένο αρχείο, ώστε να μπορεί να εγκατασταθεί κακόβουλο λογισμικό σε ένα μηχάνημα. Αυτή τη στιγμή είναι η πιο διαδεδομένη μορφή επίθεσης phishing.

SPEAR PHISHING

Ενώ οι περισσότερες επιθέσεις phishing ρίχνουν ένα ευρύ δίχτυ, ελπίζοντας να δελεάσουν όσο το δυνατόν περισσότερους χρήστες να τσιμπήσουν το δόλωμα, το spear phishing περιλαμβάνει εντατική έρευνα ενός προκαθορισμένου στόχου υψηλού κόστους, συχνά βασιζόμενο σε δημόσια διαθέσιμες πληροφορίες για ένα πιο πειστικό τέχνασμα.

Αυτό συνεπάγεται μια τεχνική, όπου ο phisher στοχεύει ένα συγκεκριμένο άτομο ή μια ομάδα ατόμων και όχι μια γενική βάση χρηστών. Αυτές οι επιθέσεις έχουν επιτυχία ακριβώς, επειδή είναι πιο εξατομικευμένες. Ο δράστης προσαρμόζει τα μηνύματα ηλεκτρονικού ταχυδρομείου με το όνομα, την εταιρεία, τον αριθμό τηλεφώνου και παρόμοιες πληροφορίες του παραλήπτη, κάνοντας τον στόχο να πιστέψει ότι μοιράζεται κάποια μορφή σύνδεσης με τον αποστολέα.

Η επιτυχής δημιουργία πειστικών ηλεκτρονικών μηνυμάτων spear-phishing απαιτεί πολύ χρόνο, καθώς ο phisher πρέπει να αποκτήσει πολλαπλά δεδομένα από διάφορες πηγές. Δεν είναι λοιπόν περίεργο ότι αυτό το είδος κακόβουλης επίθεσης είναι διαδεδομένο σε πλατφόρμες κοινωνικής δικτύωσης όπως το LinkedIn, όπου ο phisher μπορεί να χρησιμοποιήσει τακτικές κοινωνικής μηχανικής.

SMS + PHISHING = SMISHING

Απλά μην κάνετε κλικ - Το phishing με SMS χρησιμοποιεί τα μηνύματα κειμένου ως μέθοδο για την παράδοση κακόβουλων συνδέσμων, συχνά με τη μορφή σύντομων κωδικών, για να παγιδεύσει τους χρήστες smartphone. Η έλευση της κινητής τεχνολογίας επέφερε πληθώρα πλεονεκτημάτων στην επικοινωνία και τις ηλεκτρονικές τραπεζικές συναλλαγές. Ταυτόχρονα, έφερε και ένα νέο κίνδυνο για τη διάπραξη περισσότερων εγκλημάτων. Ένα από αυτά είναι το smishing, όπου οι εγκληματίες του κυβερνοχώρου δελεάζουν τα θύματα μέσω γραπτών

	μηνυμάτων, για να επισκεφθούν αθέμιτους ιστότοπους, να λάβουν κακόβουλες εφαρμογές, να επικοινωνήσουν με την τεχνική υποστήριξη. Είτε με τη μορφή ενός κωδικού κουπονιού, είτε με την προσφορά δωρεάν εισιτηρίων ή χρημάτων, μια απόπειρα smishing τις περισσότερες φορές απαιτεί να κάνετε κλικ σε έναν σύνδεσμο που σας κατευθύνει σε έναν ιστότοπο. Αρκετά συνηθισμένοι είναι επίσης οι σύνδεσμοι που ενεργοποιούν την αυτόματη λήψη επικίνδυνων εφαρμογών. Παρόλο που εμφανίζονται να προέρχονται από νόμιμες πηγές με URL που σας είναι οικείες, αποσκοπούν απλώς στην κλοπή προσωπικών πληροφοριών ή στην εγκατάσταση κακόβουλου λογισμικού στην κινητή σας συσκευή. **ΜΗΧΑΝΗ ΑΝΑΖΗΤΗΣΗΣ PHISHING** Προσέξτε τι επιλέγετε - Σε αυτόν τον τύπο επίθεσης, οι εγκληματίες του κυβερνοχώρου περιμένουν να έρθετε εσείς σε αυτούς. Το phishing σε μηχανές αναζήτησης εισάγει δόλιους ιστότοπους, συχνά με τη μορφή πληρωμένων διαφημίσεων, στα αποτελέσματα δημοφιλών όρων αναζήτησης. **VISHING** Το Vishing περιλαμβάνει έναν απατεώνα που καλεί το θύμα, προσποιούμενος ότι προέρχεται από έναν αξιόπιστο οργανισμό και προσπαθεί να αποσπάσει προσωπικές πληροφορίες, όπως τραπεζικά στοιχεία ή στοιχεία πιστωτικής κάρτας. Τις περισσότερες φορές, αυτός που καλεί στην άλλη γραμμή ακούγεται προφανώς σαν ρομπότ, αλλά καθώς η τεχνολογία εξελίσσεται, η τακτική αυτή είναι όλο και πιο δύσκολο να αναγνωριστεί. **PHARMING - Δηλητηριάζοντας την τρύπα του νερού** Γνωστό και ως DNS poisoning, το pharming είναι μια τεχνικά εξελιγμένη μορφή phishing που περιλαμβάνει το σύστημα ονομάτων τομέα (DNS) του διαδικτύου. Το pharming ανακατευθύνει τη νόμιμη διαδικτυακή κυκλοφορία σε μια παραποιημένη σελίδα χωρίς να το γνωρίζει ο χρήστης, συχνά για να υποκλέψει πολύτιμες πληροφορίες. Με το άνοιγμα της κακόβουλης ιστοσελίδας, του συνδέσμου ή του συνημμένου αρχείου, ο υπολογιστής σας φορτώνεται αυτόματα με κακόβουλο λογισμικό που εξαπλώνεται σε άλλα συστήματα εντός της εταιρείας. Για τη διαιώνιση επιτυχημένων επιθέσεων, ο χάκερ συχνά εντοπίζει τους ιστότοπους που επισκέπτεστε τακτικά και παρακολουθεί τα μοτίβα ηλεκτρονικού ταχυδρομείου. Με το pharming, ο δράστης δεν επιτίθεται σε άτομα. Αντίθετα, η επίθεση κατευθύνεται στο DNS (Domain Name System), όπου ο απατεώνας προκαλεί δηλητηρίαση της κρυφής μνήμης DNS. Αυτό αλλάζει τη διεύθυνση IP που σχετίζεται με το όνομα ενός ιστότοπου, έτσι ώστε ακόμη και όταν τα άτομα εισάγουν το σωστό όνομα ιστότοπου, ο απατεώνας μπορεί να ανακατευθύνει τους χρήστες στον κακόβουλο ιστότοπο. Αν και λιγότερο διαδεδομένη, η

	στόχευση του διακομιστή DNS θα μπορούσε να θέσει σε κίνδυνο εκατομμύρια αιτήσεις URL από χρήστες του διαδικτύου. **CLONE PHISHING** Σε αυτόν τον τύπο επίθεσης, ένας σκιώδης δράστης κάνει αλλαγές σε ένα υπάρχον μήνυμα ηλεκτρονικού ταχυδρομείου, με αποτέλεσμα ένα σχεδόν πανομοιότυπο (κλωνοποιημένο) μήνυμα ηλεκτρονικού ταχυδρομείου, αλλά με έναν νόμιμο σύνδεσμο, συνημμένο αρχείο ή άλλο στοιχείο που έχει αντικατασταθεί με ένα κακόβουλο. Αυτές οι επιθέσεις δεν μπορούν να ξεκινήσουν χωρίς ο επιτιθέμενος να έχει προηγουμένως παραβίαση ενός λογαριασμού ηλεκτρονικού ταχυδρομείου, οπότε μια καλή άμυνα είναι η χρήση ισχυρών, μοναδικών κωδικών πρόσβασης σε συνδυασμό με έλεγχο ταυτότητας δύο παραγόντων. **MAN-IN-THE-MIDDLE** Ο Phisherman του δημόσιου WiFi - Η επίθεση man-in-the-middle περιλαμβάνει έναν υποκλοπέα που παρακολουθεί την αλληλογραφία μεταξύ δύο ανυποψίαστων μερών. Όταν αυτό γίνεται με σκοπό την κλοπή διαπιστευτηρίων ή άλλων ευαίσθητων πληροφοριών, πρόκειται για επίθεση phishing man-in-the-middle. Αυτές οι επιθέσεις πραγματοποιούνται συχνά με τη δημιουργία ψεύτικων δημόσιων δικτύων WiFi σε καφετέριες, εμπορικά κέντρα και άλλες δημόσιες τοποθεσίες. Μόλις συνδεθεί, ο απατεώνας μπορεί να αλιεύσει πληροφορίες ή να προωθήσει κακόβουλο λογισμικό σε συσκευές. **MALVERTISING** Αυτή η διαφήμιση δεν είναι αυτό που νομίζετε ότι είναι – Ο συγκεκριμένος τύπος phishing εκμεταλλεύεται τις αδυναμίες του λογισμικού διαφήμισης ή animation, για να κλέψει πληροφορίες από στοχευμένους χρήστες. Η κακόβουλη διαφήμιση ενσωματώνεται συνήθως σε διαφημίσεις που κατά τα άλλα φαίνονται φυσιολογικές -και τοποθετούνται σε νόμιμες ιστοσελίδες όπως η Yahoo.com- αλλά με κακόβουλο κώδικα που εμφυτεύεται μέσα σε αυτές. **ΠΑΡΑΠΟΙΗΣΗ DOMAIN** Το δεύτερο είδος ηλεκτρονικού «ψαρέματος» εμφανίζεται με τη μορφή του domain spoofing, όπου ο δράστης παραποιεί το domain name ενός αξιόλογου οργανισμού. Με αυτή την τεχνική φαίνεται ότι λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από μια νόμιμη εταιρεία. Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου είναι μοναδικές, οπότε ο phisher μπορεί να μιμηθεί μόνο τη διεύθυνση του οργανισμού. Αυτό το επιτυγχάνει, χρησιμοποιώντας αντικατάσταση χαρακτήρων, όπως "r" και "n" μαζί για "rn" αντί για "m". Διαφορετικά, χρησιμοποιούν το όνομα του οργανισμού με διαφορετικό τομέα, με την ελπίδα ότι μόνο το τοπικό μέρος της διεύθυνσης ηλεκτρονικού ταχυδρομείου θα εμφανιστεί στα εισερχόμενα του παραλήπτη. Μια παραποίηση domain μπορεί επίσης να δημιουργήσει έναν δόλιο ιστότοπο που μοιάζει με τον πραγματικό. Αντιγράφεται ο σχεδιασμός του πραγματικού ιστότοπου. Για άλλη μια φορά, η

	έμφαση δίνεται στη φράση «μοιάζει». Ενώ ο ψεύτικος τομέας μπορεί να είναι παρόμοιος, δεν είναι πανομοιότυπος με τον αρχικό ιστότοπο. **EVIL TWIN** Στα σημεία πρόσβασης WI-FI μπαίνουν πολλοί χρήστες, που αναζητούν γρήγορες ασύρματες συνδέσεις, για να σερφάρουν στο διαδίκτυο και να εκτελούν άλλες δραστηριότητες που βασίζονται στο διαδίκτυο. Ο χάκερ σε αυτό το σενάριο αντιγράφει το σημείο πρόσβασης WI-FI με ένα ψεύτικο. Όταν οι χρήστες συνδέονται, ο χάκερ είναι σε θέση να κρυφακούσει την κυκλοφορία του δικτύου τους. Κλέβει ονόματα λογαριασμών και κωδικούς πρόσβασης. Ο επιτήδειος είναι επίσης σε θέση να βλέπει τυχόν συνημμένα αρχεία στα οποία ο χρήστης αποκτά πρόσβαση, ενώ βρίσκεται στο παραβιασμένο δίκτυο. Τα ευάλωτα σημεία πρόσβασης WI-FI περιλαμβάνουν εκείνα σε καφετέριες, αεροδρόμια, εμπορικά κέντρα, νοσοκομεία και άλλες δημόσιες τοποθεσίες hotspot. **Παραδείγματα επιθέσεων Phishing σε πραγματικές συνθήκες** Σύμφωνα με πρόσφατη έρευνα της Google, από τον Ιανουάριο έως τον Μάρτιο του 2020 σημειώθηκε αύξηση κατά 3505 των ιστοσελίδων phishing. Μια άλλη έρευνα της Check Point Research αποκάλυψε ότι το 64% των επιχειρήσεων τον τελευταίο χρόνο είχαν πέσει θύματα επιθέσεων phishing. Περισσότερα ευρήματα της Verizon επιβεβαίωσαν ότι το phishing εμπλέκεται στο 78% των περιστατικών κυβερνο-κατασκοπείας. Αυτά είναι πέντε από τα πιο αξιοσημείωτα παραδείγματα: Το whaling attack οδηγεί στην απόλυση του αφεντικού της FACC Το 2016, η αυστριακή εταιρεία αεροδιαστημικής FACC είχε υποστεί μια από τις πιο γνωστές επιθέσεις whaling που έγιναν ποτέ, η οποία ονομάστηκε Fake President Incident, όπου ο επιτιθέμενος απέσπασε 56 εκατομμύρια δολάρια. Σε μια κλασική επίθεση αυτού του τύπου, ο δράστης υποδύθηκε τον διευθύνοντα σύμβουλο και στέλνοντας ένα μήνυμα ηλεκτρονικού ταχυδρομείου σε έναν υπάλληλο του οικονομικού τμήματος ζήτησε την άμεση μεταφορά χρημάτων. Η επίθεση δεν κόστισε μόνο οικονομικές απώλειες στην εταιρεία, αλλά και τη θέση του τότε διευθύνοντος συμβούλου, Walter Stephan. Αν και οι λεπτομέρειες δεν αποκαλύφθηκαν, η απόλυση έγινε λόγω παραβίασης των καθηκόντων του. **Spear Phishing με στόχο την Ubiquiti Networks Inc.** Τον Ιούνιο του 2015, η αμερικανική εταιρεία τεχνολογίας δικτύων Ubiquiti Networks έγινε στόχος spear-phishing. Ο επιτιθέμενος παρίστανε υψηλόβαθμα στελέχη από ένα υποκατάστημα στο εξωτερικό με παραποιημένες διευθύνσεις ηλεκτρονικού ταχυδρομείου και παραλλαγές domain. Οι υπάλληλοι ξεγελάστηκαν και πίστεψαν ότι έλαβαν νόμιμα αιτήματα από στελέχη της εταιρείας για μεταφορά χρημάτων σε έναν ασφαλή λογαριασμό. Η Ubiquiti Networks δεν γνώριζε ότι είχε πέσει θύμα απάτης μέχρι που ενημερώθηκε για τη δραστηριότητα από το FBI. Δεν υπέστη καμία παραβίαση των συστημάτων της, έχασε 46,7 εκατομμύρια δολάρια από τα μεταφερόμενα κεφάλαια.

Απάτη με τιμολόγια Facebook και Google

Μεταξύ του 2013 και του 2015, οι αμερικανικές εταιρείες-κολοσσοί Facebook και Google φέρεται να εξαπατήθηκαν με 100 εκατομμύρια δολάρια σε ένα περίτεχνο σχέδιο απάτης μέσω τηλεγραφημάτων. Ο δράστης δημιούργησε μια ψεύτικη επιχείρηση που παρίστανε την ταϊβανέζικη εταιρεία Quanta Computer. Η τελευταία πραγματοποιούσε τακτικά συναλλαγές πολλών εκατομμυρίων δολαρίων με τις εταιρείες μέσων κοινωνικής δικτύωσης και κατά τη διάρκεια των δύο ετών, ο επιτιθέμενος έστελνε ηλεκτρονικά μηνύματα phishing με πλαστά τιμολόγια που έπρεπε να καταβληθούν σε ψεύτικους τραπεζικούς λογαριασμούς. Το σύστημα απέφυγε τις υποψίες για τόσο μεγάλο χρονικό διάστημα δημιουργώντας ψεύτικα δικαιολογητικά για τις συναλλαγές και πλαστογραφώντας εταιρικές σφραγίδες. Ο επιτιθέμενος ταυτοποιήθηκε αργότερα ως ο Λιθουανός Evaldas Rimasauskas, στον οποίο επιβλήθηκε ποινή φυλάκισης πέντε ετών μετά τη σύλληψή του το 2017.

Apple Smishing

Το 2020, μια από τις μεγαλύτερες εταιρείες smartphone στον κόσμο, η Apple, έγινε στόχος μιας εκστρατείας smishing. Με ένα ψεύτικο πλαίσιο συνομιλίας της Apple, τα μηνύματα ενημέρωναν τους χρήστες ότι είχαν την ευκαιρία να συμμετάσχουν στο πρόγραμμα δοκιμών της Apple 2020 για το νέο iPhone 12. Οι παραλήπτες κλήθηκαν να πληρώσουν μια χρέωση παράδοσης. Οδηγούνταν σε έναν κακόβουλο ιστότοπο, μέσω του οποίου οι επιτιθέμενοι υπέκλεπταν τα στοιχεία της κάρτας πληρωμής των θυμάτων. Οι άνθρωποι στις μέρες μας διατηρούν πολλές ευαίσθητες πληροφορίες στα smartphones τους και η ευρεία χρήση των iPhone και iPad τα έχει καταστήσει επαναλαμβανόμενους στόχους για συστήματα SMS phishing. Οι επιτιθέμενοι στέλνουν τακτικά μηνύματα στους χρήστες. Τα μηνύματα αυτά περιέχουν έναν σύνδεσμο που πρέπει να ακολουθήσουν, για να ξεκλειδώσουν έναν δεσμευμένο λογαριασμό Apple ID ή για να αποτρέψουν τη λήξη του από μελλοντικά μηνύματα αυτού του είδους. Άλλα θα δελεάσουν τους χρήστες με την ιδέα ότι βρέθηκε ένα χαμένο iPhone. Τα θύματα εξαπατώνται με τα διαπιστευτήρια σύνδεσής τους και οι χάκερ αποκτούν πρόσβαση στα πολυμέσα, τα έγγραφα και άλλες πληροφορίες που είναι αποθηκευμένα στη συσκευή. Ως συνεχής απειλή, το ποσό που χάνεται κατά τις επιτυχείς απόπειρες προστίθεται στις στατιστικές για τις ετήσιες απώλειες από το έγκλημα στον κυβερνοχώρο. Παρόλο που δεν πέφτουν όλοι θύματα, ο επιτιθέμενος κερδίζει σημαντικές ανταμοιβές για το μικρό ποσοστό των ανθρώπων που εξαπατά.

Παραβίαση ασφάλειας RSA

Το μόνο που χρειάστηκε ένας εισβολέας, για να αποκτήσει πρόσβαση στο σύστημα δικτύου της δημοφιλούς εταιρείας κυβερνοασφάλειας ήταν ένα μήνυμα ηλεκτρονικού ταχυδρομείου με θέμα «Σχέδιο πρόσληψης 2011». Στο μήνυμα ηλεκτρονικού ταχυδρομείου υπήρχε ένα μολυσμένο από ιό αρχείο Excel, και μόλις το άνοιξε ένας ανυποψίαστος υπάλληλος έδωσε στον εισβολέα πρόσβαση σε ιδιωτικούς κωδικούς πρόσβασης.

	Κατά ειρωνικό τρόπο, η RSA παρέχει υπηρεσίες κυβερνοασφάλειας σε διάφορους κλάδους της αμερικανικής κυβέρνησης και σε άλλες επιχειρήσεις. Η παραβίαση αυτή έδωσε στους χάκερς πρόσβαση στα δίκτυα των κυβερνητικών υπηρεσιών των ΗΠΑ, αποτελώντας μια προηγμένη μόνιμη απειλή. Δείτε αυτό το βίντεο https://www.youtube.com/watch?v=4AcROYO8BLA
Εμπόδια/δυσκολίες για ενήλικες	Τα μηνύματα ηλεκτρονικού ταχυδρομείου, τα μηνύματα κειμένου, τα μηνύματα φωνητικού ταχυδρομείου, ακόμη και οι φωνητικές κλήσεις δεν πιστοποιούνται. Αυτό σημαίνει ότι, όπως ακριβώς και μια καρτ ποστάλ που αποστέλλεται μέσω ταχυδρομείου, δεν υπάρχει πραγματικός τρόπος να επικυρωθεί από πού προέρχονται. Αυτό δίνει στους απατεώνες μεγάλη ελευθερία να μιμούνται αξιόπιστες μάρκες στις επικοινωνίες τους. Το phishing είναι μία από τις πιο κοινές και διαδεδομένες απειλές. Οι εξελιγμένοι phishers είναι πολύ επιδέξιοι στο να δημιουργούν ψεύτικα πρότυπα email και ιστότοπους που είναι σχεδόν δυσδιάκριτοι από τους πραγματικούς, μέχρι και τη διεύθυνση URL (διεύθυνση ιστότοπου) και τα πιστοποιητικά ασφαλείας. Μπορεί να νομίζετε ότι λαμβάνετε ένα αξιόπιστο μήνυμα από μια τράπεζα, ένα ηλεκτρονικό κατάστημα ή μια εταιρεία πιστωτικών καρτών. Και αν δεν δίνετε μεγάλη προσοχή, μπορεί να μην αντιληφθείτε την απάτη μέχρι να είναι πολύ αργά.
Κίνδυνος των κοινωνικών μέσων/εργαλείων στους ενήλικες	Σύμφωνα με τη Wikipedia, το phishing είναι μια δόλια απόπειρα απόκτησης ευαίσθητων δεδομένων με τον χάκερ να προσποιείται ότι είναι μια αξιόπιστη οντότητα. Όπως και κάθε άλλο είδος απάτης, ο δράστης μπορεί να προκαλέσει σημαντική ζημιά, ειδικά όταν η απειλή επιμένει για μεγάλο χρονικό διάστημα. Όπως και σε κάθε άλλο είδος απάτης, ο δράστης μπορεί να προκαλέσει σημαντική ζημιά, ιδίως όταν η απειλή επιμένει για μεγάλο χρονικό διάστημα. Η απάτη μέσω ηλεκτρονικού ταχυδρομείου έχει έναν κατάλογο αρνητικών συνεπειών, όπως απώλεια χρημάτων, απώλεια πνευματικής ιδιοκτησίας, βλάβη της φήμης, μερικές φορές με ανεπανόρθωτες επιπτώσεις. Αν και οι ηλικιακά μεγαλύτεροι σπάνια αναφέρουν ότι πέφτουν θύματα οικονομικού ηλεκτρονικού εγκλήματος, υπάρχουν στοιχεία που δείχνουν ότι διατρέχουν αυξημένο κίνδυνο. Σύμφωνα με την έρευνα, η κοινωνική απομόνωση, τα γνωστικά, σωματικά και ψυχικά προβλήματα υγείας, η περιουσιακή κατάσταση, οι περιορισμένες δεξιότητες ή η ευαισθητοποίηση στον τομέα της ασφάλειας στον κυβερνοχώρο, οι κοινωνικές συμπεριφορές και το περιεχόμενο των απατών οδηγούν στη θυματοποίηση. Η οικονομική απώλεια για τα θύματα μεγαλύτερης ηλικίας ήταν σχεδόν διπλάσια ανά απάτη σε σχέση με τα νεότερα θύματα Ωστόσο, είναι σημαντικό να σημειωθεί ότι η οικονομική απώλεια για τα θύματα μεγαλύτερης ηλικίας (ηλικίας 55 ετών και άνω) ήταν πιθανό να είναι σχεδόν διπλάσια ανά απάτη σε σχέση με τις νεότερες ηλικιακές ομάδες. Επίσης, μπορεί να υποτεθεί ότι, για πολλούς ηλικιωμένους με σταθερό εισόδημα (και χωρίς εύκολα μέσα δημιουργίας νέων αποταμιεύσεων για παράδειγμα), είναι πιθανόν πιο δύσκολο να

	αντικαταστήσουν τα χρήματα που χάθηκαν ως αποτέλεσμα απάτης απ' ό,τι για τα άτομα σε ηλικία εργασίας. Σχεδόν το ήμισυ (49%) του συνόλου των ατόμων ηλικίας 75 ετών και άνω ζουν μόνα τους και το 17% των ηλικιακά μεγαλύτερων έχουν λιγότερες εβδομαδιαίες επαφές με την οικογένεια, τους φίλους και τους γείτονες. Τα άτομα που είναι περισσότερο κοινωνικά απομονωμένα μπορεί κάλλιστα να είναι πιο ευάλωτα στην απάτη, για παράδειγμα, αν έχουν λίγες ευκαιρίες να συζητήσουν τα θέματα με άλλους. **Πώς οι ηλικιακά μεγαλύτεροι πέφτουν θύματα του phishing;** Η εξαπάτηση των ηλικιακά μεγαλύτερων είναι ένα τεράστιο πρόβλημα σε όλο τον κόσμο. Οι απάτες που ξεκινούν από το Διαδίκτυο γίνονται όλο και πιο συχνές και σε αυτόν τον πληθυσμό, ιδίως καθώς οι ηλικιακά μεγαλύτεροι που γνωρίζουν το Διαδίκτυο αρχίζουν να γερνούν. **Εάν έχετε ανταποκριθεί σε μια απάτη phishing, ο επιτιθέμενος μπορεί ενδεχομένως:** Να καταχραστεί το όνομα χρήστη και τον κωδικό σας Να κλέψει τα χρήματά σας και να ανοίξει πιστωτικές κάρτες και τραπεζικούς λογαριασμούς στο όνομά σας Να ζητήσει νέους προσωπικούς αριθμούς αναγνώρισης (PIN) λογαριασμού ή πρόσθετες πιστωτικές κάρτες Να πραγματοποιήσει αγορές Να προσθέσει τον εαυτό του ή έναν σύμμαχο που είναι εξουσιοδοτημένος χρήστης, ώστε να είναι ευκολότερη η χρήση της κάρτας σας. Να λάβει προκαταβολές Να καταχραστεί τον Αριθμό Κοινωνικών Ασφαλίσεών σας Να πουλήσει τις πληροφορίες σας σε άλλους που θα τις χρησιμοποιήσουν για παράνομους σκοπούς. Πώς με εντόπισε μια απάτη phishing; Αυτό το είδος κλοπής ταυτότητας είναι εξαιρετικά διαδεδομένο λόγω της ευκολίας με την οποία ανυποψίαστοι άνθρωποι μοιράζονται προσωπικές πληροφορίες. Οι απάτες phishing συχνά σας δελεάζουν με μηνύματα ηλεκτρονικού ταχυδρομείου spam και στιγμιαία μηνύματα που σας ζητούν να «επαληθεύσετε τον λογαριασμό σας» ή να «επιβεβαιώσετε τη διεύθυνση χρέωσης» μέσω ενός κακόβουλου ιστότοπου. Να είστε πολύ προσεκτικοί. Οι Phishers μπορούν να σας βρουν μόνο αν ανταποκριθείτε. **Πώς θα καταλάβω αν έχω πέσει θύμα ηλεκτρονικού «ψαρέματος»;** Οι Phishers συχνά προσποιούνται ότι είναι νόμιμες εταιρείες. Τα μηνύματά τους μπορεί να ακούγονται γνήσια και οι ιστοσελίδες τους μπορεί να μοιάζουν εντυπωσιακά με τις πραγματικές. Μπορεί να είναι δύσκολο να καταλάβετε τη διαφορά, αλλά αν δείτε τα εξής μπορεί να καταλάβετε ότι είναι απάτη:

	Αιτήματα για εμπιστευτικές πληροφορίες μέσω ηλεκτρονικού ταχυδρομείου ή άμεσων μηνυμάτων Συναισθηματική γλώσσα που χρησιμοποιεί τακτικές εκφοβισμού ή επείγοντα αιτήματα για ανταπόκριση Λανθασμένες διευθύνσεις URL, ορθογραφικά λάθη ή χρήση υπο-τομέων Σύνδεσμοι εντός ενός μηνύματος Έλλειψη προσωπικού χαιρετισμού ή εξατομικευμένων πληροφοριών εντός ενός μηνύματος. Τα νόμιμα μηνύματα ηλεκτρονικού ταχυδρομείου από τράπεζες και εταιρείες πιστωτικών καρτών συχνά περιλαμβάνουν μερικούς αριθμούς λογαριασμού, όνομα χρήστη ή κωδικό πρόσβασης. **Επιπτώσεις** **Απώλεια χρημάτων** Από κάθε περιστατικό phishing που έχει λάβει χώρα, ένα κοινό αποτέλεσμα είναι η οικονομική απώλεια. Οι οικονομικές απώλειες που υφίστανται οι μεμονωμένοι καταναλωτές εκτιμάται ότι ξεπερνούν τα 9 δισεκατομμύρια λίρες ετησίως. Ωστόσο, αν και τα στοιχεία αυτά αποτελούν χρήσιμους δείκτες, είναι πιθανό να υποεκτιμούν σημαντικά την κλίμακα των οικονομικών απωλειών που υφίστανται οι ιδιώτες, καθώς δεν φαίνεται να περιλαμβάνουν όλους τους τύπους απάτης και, όπως αναφέρεται, πολλά αδικήματα απάτης δεν καταγγέλλονται. Συγκεχυμένα, το ποσό των 3,5 δισεκατομμυρίων λιρών αναφέρεται επίσης συχνά ως εκτίμηση των συνολικών οικονομικών απωλειών που υπέστησαν οι άνθρωποι ως αποτέλεσμα απάτης. **Άλλες επιπτώσεις** Γενικά, οι άλλες επιπτώσεις της απάτης για τα θύματα μπορεί να ποικίλλουν ανάλογα με τις ατομικές συνθήκες των ατόμων και τους υπάρχοντες πόρους και τις δυνατότητές τους, αλλά η σοβαρότητα των πιθανών επιπτώσεων δεν πρέπει ποτέ να υποτιμάται. Οι ψυχολογικές επιπτώσεις μπορεί να είναι σοβαρές και εξουθενωτικές, όπως άγχος, θυμός, απώλεια αυτοεκτίμησης, ντροπή και αναστάτωση. Ο αρνητικός αντίκτυπος της οικονομικής κακοποίησης, ανεξάρτητα από την πηγή της, μπορεί να έχει ως αποτέλεσμα κάποιος να έχει ανάγκη υποστήριξης από τις κοινωνικές υπηρεσίες, ενώ προηγουμένως δεν χρειαζόταν τέτοια βοήθεια. Μια μελέτη για το έγκλημα κατ' οίκον έδειξε ότι η υγεία των θυμάτων μειώνεται ταχύτερα από ό,τι των μη θυμάτων παρόμοιας ηλικίας. Η ανάλυση των επιπτώσεων του εγκλήματος κατ' οίκον διαπίστωσε ότι: Το 40% των θυμάτων δήλωσαν ότι αυτό είχε ως αποτέλεσμα να μειωθεί η εμπιστοσύνη τους γενικά. Το 28% δήλωσε ότι αισθάνονταν πεσμένοι ή καταθλιπτικοί. Το 46% δήλωσε ότι τους προκάλεσε οικονομική ζημιά. Το 16% δεν είχε μιλήσει σε κανέναν για το έγκλημα, και το 40% αυτών δήλωσε ότι ο λόγος ήταν η αμηχανία.

	Τα θύματα είναι συχνά ευάλωτα άτομα που μπορεί να βρίσκονται σε οικονομική δυσπραγία ή είναι ηλικιωμένα ή κοινωνικά απομονωμένα. Ο προσωπικός αντίκτυπος σε αυτούς και στις οικογένειές τους είναι συχνά καταστροφικός όσον αφορά τη μελλοντική ψυχική ηρεμία και υγεία τους. Τα θύματα μπορεί να χάσουν την αυτοεκτίμησή τους και να υποφέρουν από στρες, άγχος και κατάθλιψη. Οι ζωές τους μπορεί να καταστραφούν. Σχεδόν το ήμισυ (49%) του συνόλου των ατόμων ηλικίας 75 ετών και άνω ζουν μόνα τους και το 17% των ηλικιακά μεγαλύτερων έχουν λιγότερες από εβδομαδιαίες επαφές με την οικογένεια, τους φίλους και τους γείτονες. Τα άτομα που είναι περισσότερο κοινωνικά απομονωμένα μπορεί κάλλιστα να είναι πιο ευάλωτα στην απάτη, για παράδειγμα, αν έχουν λίγες ευκαιρίες να συζητήσουν τα θέματα με άλλους. Πώς οι ηλικιακά μεγαλύτεροι πέφτουν θύματα του phishing;
Λύσεις που μπορούμε να έχουμε	Η καλύτερη άμυνα απέναντι σε μια απάτη phishing είναι να επαληθεύετε με το άτομο ή τους οργανισμούς που έστειλαν το email ή το μήνυμα πριν κάνετε κλικ σε οτιδήποτε. **Πώς μπορείτε να προστατευτείτε από το phishing;** Όταν οπλίζεστε με πληροφορίες και πόρους, είστε σοφότεροι σχετικά με τις απειλές για την ασφάλεια των υπολογιστών και λιγότερο ευάλωτοι σε τακτικές απάτης phishing. Ακολουθήστε αυτά τα βήματα για να ενισχύσετε την ασφάλεια του υπολογιστή σας και να αποκτήσετε αμέσως καλύτερη προστασία από το phishing: Μην παρέχετε προσωπικές πληροφορίες σε αυθαίρετες αιτήσεις για πληροφορίες. Παρέχετε προσωπικές πληροφορίες μόνο σε ιστότοπους που έχουν "https" στη διεύθυνση ιστού ή έχουν ένα εικονίδιο κλειδαριάς στο κάτω μέρος του προγράμματος περιήγησης. Εάν υποψιάζεστε ότι έχετε πέσει θύμα phishing, επικοινωνήστε τηλεφωνικά με την εταιρεία που υποτίθεται έστειλε το email, για να ελέγξετε ότι το μήνυμα είναι νόμιμο. Πληκτρολογήστε μια αξιόπιστη διεύθυνση URL για τον ιστότοπο μιας εταιρείας, για να την συγκρίνετε με το ύποπτο μήνυμα ηλεκτρονικού «ψαρέματος». Χρησιμοποιήστε ποικίλους και σύνθετους κωδικούς πρόσβασης για όλους τους λογαριασμούς σας. Να ελέγχετε συνεχώς την ακρίβεια των προσωπικών λογαριασμών και να αντιμετωπίζετε αμέσως τυχόν αποκλίσεις. Αποφύγετε αμφισβητήσιμους ιστότοπους. Εφαρμόστε ασφαλές πρωτόκολλο ηλεκτρονικού ταχυδρομείου: Μην ανοίγετε μηνύματα από άγνωστους αποστολείς Διαγράψτε αμέσως τα μηνύματα που υποψιάζεστε ότι είναι ανεπιθύμητα.

	Βεβαιωθείτε ότι έχετε εγκαταστήσει τα καλύτερα προϊόντα λογισμικού ασφαλείας στον υπολογιστή σας για καλύτερη προστασία από το phishing: Χρησιμοποιήστε λογισμικό προστασίας από ιούς και πρόγραμμα προστασίας. Αποκτήστε προστασία από λογισμικό antispyware. Ένας απροστάτευτος υπολογιστής είναι σαν μια ανοιχτή πόρτα για απάτες ηλεκτρονικού «ψαρέματος». Για μια πιο ισχυρή μορφή προστασίας, χρησιμοποιήστε ένα φίλτρο ανεπιθύμητης αλληλογραφίας ή μια πύλη για τη σάρωση των εισερχόμενων μηνυμάτων. Αυτά τα προϊόντα αποτρέπουν επικίνδυνα κακόβουλα προγράμματα πριν εισέλθουν στον υπολογιστή σας, στέκονται φρουροί σε κάθε πιθανή είσοδο του υπολογιστή σας και αποκρούουν κάθε λογισμικό κατασκοπείας ή ιό που προσπαθεί να εισέλθει, ακόμη και τα πιο επιζήμια και ύπουλα. Ενώ υπάρχουν διαθέσιμες δωρεάν λήψεις anti-spyware και antivirus, απλά δεν μπορούν να συμβαδίσουν με τη συνεχή επίθεση νέων στελεχών spyware. Οι προηγουμένως μη εντοπισμένες μορφές spyware μπορούν συχνά να προκαλέσουν τη μεγαλύτερη ζημιά, γι' αυτό είναι ζωτικής σημασίας να διαθέτετε ενημερωμένη και εγγυημένη προστασία. **Συγκρίνετε & βρείτε το καλύτερο λογισμικό προστασίας από Phishing** Οι διαδικτυακοί απατεώνες θα προσπαθήσουν να σας ξεγελάσουν και να σας αναγκάσουν να παραδώσετε τους κωδικούς πρόσβασης ή άλλες προσωπικές πληροφορίες σας, εμφανιζόμενοι ως νόμιμοι ιστότοποι. Συχνά, μάλιστα, ενεργούν όπως οι ιστότοποι στους οποίους συνδέεστε τακτικά. Αυτές οι απειλές αποφεύγονται εύκολα με ένα πρόγραμμα προστασίας από ιούς σε λειτουργία. Είναι χαρά μας να σας δείξουμε ποια από αυτά παρέχουν την καλύτερη προστασία από τις επιθέσεις phishing χωρίς να επηρεάζουν την απόδοση του υπολογιστή σας ή να εμποδίζουν την εργασία σας. **Ποια είναι η καλύτερη λύση Antivirus;** Η Bitdefender, η μάρκα antivirus που εμπιστεύονται πάνω από 500 εκατομμύρια χρήστες σε 150 χώρες, είναι ένας από τους κορυφαίους παρόχους παγκοσμίως προϊόντων κυβερνο-ασφάλειας για καταναλωτές και πρωτοπόρος στην προστασία από ιούς. Αυτή η μάρκα έχει κερδίσει πολλαπλά βραβεία antivirus από κορυφαία εργαστήρια δοκιμών στο διαδίκτυο, συμπεριλαμβανομένων των AV-Comparatives, AV-Test, PCMag και The Anti-Malware Testing Standard Organization. Η υπηρεσία αντιμέτρων της Netcraft βοηθά τους οργανισμούς να καταπολεμήσουν αυτές τις τεχνικές. Μόλις εντοπιστεί ένας ιστότοπος phishing, η Netcraft ανταποκρίνεται αμέσως με ένα σύνολο ενεργειών που θα περιορίσουν σημαντικά την πρόσβαση στον ιστότοπο και θα προκαλέσουν τελικά την εξάλειψη του δόλιου περιεχομένου. Η προσέγγιση της Netcraft για την απομάκρυνση των phishing sites διακρίνεται από άλλους παρόχους υπηρεσιών απομάκρυνσης χάρη στην ικανότητά της να αποκλείει αμέσως την πρόσβαση στον ιστότοπο για χρήστες ενός ευρέος φάσματος τεχνολογιών.

	Τα καλύτερα λογισμικά Anti-Phishing Οι διαδικτυακοί απατεώνες θα προσπαθήσουν να σας ξεγελάσουν και να σας αναγκάσουν να δώσετε τους κωδικούς πρόσβασης ή άλλες προσωπικές πληροφορίες σας, εμφανιζόμενοι ως νόμιμοι ιστότοποι. Συχνά, μάλιστα, ενεργούν όπως οι ιστότοποι στους οποίους συνδέεστε τακτικά. Αυτές οι απειλές αποφεύγονται εύκολα με ένα πρόγραμμα προστασίας από ιούς σε λειτουργία. Είναι χαρά μας να σας δείξουμε ποια από αυτά παρέχουν την καλύτερη προστασία από τις επιθέσεις phishing χωρίς να επηρεάζουν την απόδοση του υπολογιστή σας ή να εμποδίζουν την εργασία σας. **Πιστοποιητικά επαληθευμένων σημάτων;** Τα Πιστοποιητικά Επαληθευμένου Σήματος (VMC) σας επιτρέπουν να εμφανίζετε το λογότυπό σας δίπλα στο πεδίο «αποστολέας» σε προγράμματα ηλεκτρονικού ταχυδρομείου, ώστε οι χρήστες να βλέπουν το σήμα σας -και ότι ο οργανισμός σας έχει πιστοποιηθεί- πριν καν ανοίξουν το μήνυμά σας. Πρόκειται για το ισοδύναμο του ηλεκτρονικού ταχυδρομείου με ένα σημάδι ελέγχου στα μέσα κοινωνικής δικτύωσης, με πρόσθετες απαιτήσεις επικύρωσης και ασφάλειας που συμβάλλουν στην προστασία των πελατών σας και της μάρκας σας από επιθέσεις phishing και πλαστογράφησης. Το ηλεκτρονικό ταχυδρομείο με επαλήθευση λογότυπου αποτελεί μέρος μιας πρωτοποριακής πρωτοβουλίας -σε συνεργασία με το Brand Indicators for Message Identification (BIMI) και τους παρόχους προγραμμάτων-πελατών ηλεκτρονικού ταχυδρομείου- για την προώθηση μιας συνεπούς, αξιόπιστης και οπτικά αναγνωρίσιμης εμπειρίας ηλεκτρονικού ταχυδρομείου τόσο για τις επιχειρήσεις όσο και για τους καταναλωτές. Ακούστε πώς λειτουργεί: (δείτε το βίντεο) https://www.digicert.com/content/dam/digicert/videos/digicert-vmc-product-reveal.mp4 **ΠΩΣ ΝΑ ΠΡΟΣΤΑΤΕΥΤΕΙΤΕ ΑΠΟ ΕΠΙΘΕΣΕΙΣ PHISHING** Η προστασία σας από επιθέσεις phishing ξεκινά με το να γνωρίζετε τι υπάρχει εκεί έξω. Ποτέ μην κάνετε κλικ σε συνδέσμους από άγνωστους αποστολείς ή αν οποιαδήποτε λεπτομέρεια σχετικά με την ανταλλαγή έχει προκαλέσει υποψίες. Όποτε είναι δυνατόν, περάστε με το ποντίκι πάνω από έναν σύνδεσμο για να βεβαιωθείτε ότι ανταποκρίνεται στις προσδοκίες σας. Σημειώστε ότι αυτό δεν θα λειτουργήσει στα κινητά ή αν χρησιμοποιούνται σύντομοι κωδικοί, οπότε να είστε ιδιαίτερα προσεκτικοί στις κινητές συσκευές. Αν υποψιάζεστε ότι ένα μήνυμα ηλεκτρονικού ταχυδρομείου είναι απόπειρα ηλεκτρονικού «ψαρέματος», ελέγξτε διπλά το όνομα του αποστολέα, την ιδιαιτερότητα του χαιρετισμού και το υποσέλιδο για τη φυσική διεύθυνση και το κουμπί διαγραφής. Σε περίπτωση αμφιβολίας, διαγράψτε το. Αν δεν είστε σίγουροι αν μια επικοινωνία είναι νόμιμη, προσπαθήστε να επικοινωνήσετε με την μάρκα ή την υπηρεσία μέσω άλλου καναλιού (για

	παράδειγμα, μέσω της ιστοσελίδας τους ή καλώντας την γραμμή εξυπηρέτησης πελατών). Αποφύγετε να εισάγετε προσωπικά αναγνωρίσιμες πληροφορίες, εκτός εάν είστε εξαιρετικά σίγουροι για την ταυτότητα αυτού με το οποίο επικοινωνείτε. Η επαγρύπνηση θα κρατήσει τους περισσότερους απατεώνες μακριά, αλλά κανείς δεν μπορεί να είναι 100% ασφαλής. Εξάλλου, το phishing υπάρχει σήμερα μόνο επειδή λειτουργεί. Αυτός είναι ο λόγος για τον οποίο είναι σημαντικό να συνδυάσετε την ευαισθητοποίησή σας σε θέματα ασφάλειας με την ποιοτική προστασία των τελικών σημείων των επιχειρήσεων - με βελτιωμένη νοημοσύνη απειλών με τεχνητή νοημοσύνη, ενημερώσεις που βασίζονται στο cloud και προστασία κατά του phishing-DNS σε πραγματικό χρόνο, καθώς και αξιόπιστα αντίγραφα ασφαλείας δεδομένων. **Για να αποτρέψετε τις απάτες των ηλικιακά μεγαλύτερων ατόμων;** Εάν ανησυχείτε για απάτη, μπορείτε να κάνετε πολλά για να αποτρέψετε το ενδεχόμενο να σας συμβεί: Ρυθμίστε την παρακολούθηση της πιστοληπτικής ικανότητας και την προστασία από κλοπή ταυτότητας - Οι εγκληματίες διαπράττουν σχεδόν πάντα απάτες σε ηλικιωμένους με σκοπό το οικονομικό όφελος. Ο ευκολότερος τρόπος για να προστατεύσετε τον εαυτό σας ή τα οικονομικά του αγαπημένου σας προσώπου είναι να εγγραφείτε σε πρόγραμμα παρακολούθησης της πίστωσης. **Περαιτέρω βήματα που πρέπει να ακολουθήσετε:** ΣΤΑΜΑΤΗΣΤΕ: Πάρτε μια ανάσα και σκεφτείτε την κατάσταση. Σας φαίνεται κάτι ύποπτο; ΦΥΓΕΤΕ: Κλείστε το τηλέφωνο, κλείστε την πόρτα ή κλείστε το ηλεκτρονικό ταχυδρομείο. Αν κάποιος σας πιέζει να ενεργήσετε τώρα, μπορεί να είναι απατεώνας. ΡΩΤΗΣΤΕ: Καλέστε ένα μέλος της οικογένειας για συμβουλές, αναζητήστε περισσότερες λεπτομέρειες στο διαδίκτυο και μάθετε αν οι οργανώσεις είναι πραγματικές. Μπορείτε επίσης να ζητήσετε από έναν επισκέπτη την ταυτότητά του. ΠΕΡΙΜΕΝΕΤΕ: Αφιερώστε χρόνο για να αφομοιώσετε όσα μάθατε και να καταστρώσετε ένα σχέδιο δράσης. Μην βιάζεστε να πάρετε αποφάσεις. ΔΡΑΣΗ: Επισκεφθείτε μόνο νόμιμους ιστότοπους και καλέστε επαληθευμένους, ασφαλείς τηλεφωνικούς αριθμούς. Μπορείτε να χρησιμοποιήσετε ανεξάρτητες ιστοσελίδες αναθεώρησης και υπηρεσίες αναζήτησης διευθύνσεων ηλεκτρονικού ταχυδρομείου για να ελέγξετε την ταυτότητα κάποιου. Μοιραστείτε τις ιστορίες σας για απόπειρες απάτης. Ζητήστε από τα πιο εξοικειωμένα με την τεχνολογία μέλη της οικογένειάς σας να μοιραστούν παραδείγματα μηνυμάτων ηλεκτρονικού ταχυδρομείου ή μηνυμάτων απάτης που έχουν λάβει.

	Έχετε ένα σχέδιο και έναν κωδικό πρόσβασης - Η έγκαιρη κοινοποίηση των στοιχείων του τραπεζικού λογαριασμού μπορεί να διασφαλίσει ότι τα χρήματα της οικογένειάς σας παραμένουν ασφαλή. Να είστε καχύποπτοι απέναντι σε κάθε ανεπιθύμητη κλήση ή μήνυμα - Λίγη καχυποψία μπορεί να σας γλιτώσει από μεγάλη στενοχώρια. Να γνωρίζετε ότι αυτές οι απάτες υπάρχουν και να αναρωτιέστε πάντα «τι θα γινόταν αν;» όταν έρχεστε αντιμέτωποι με ένα ασυνήθιστο αίτημα για χρήματα είτε διαδικτυακά είτε προσωπικά.

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**FACEBOOK**
Γενικές πληροφορίες	Το Facebook είναι μια αμερικανική διαδικτυακή υπηρεσία κοινωνικής δικτύωσης που ανήκει στην Meta Platforms. Ιδρύθηκε το 2004 και το όνομά της προέρχεται από τους καταλόγους - face book (https://en.wikipedia.org/wiki/Face_book) που δίνονται συχνά σε Αμερικανούς φοιτητές πανεπιστημίων. Στην αρχή η συμμετοχή περιοριζόταν μόνο σε φοιτητές του Χάρβαρντ. Από το 2006, ήταν διαθέσιμο για οποιονδήποτε άνω των 13 ετών. Ήταν η εφαρμογή για κινητά με τις περισσότερες λήψεις. Αυτή τη στιγμή το Facebook είναι προσβάσιμο από διαφορετικούς τύπους συσκευών που διαθέτουν σύνδεση στο Διαδίκτυο. Μπορείτε εύκολα να το χρησιμοποιήσετε σε προσωπικούς υπολογιστές, tablet και smartphones. Για να χρησιμοποιήσετε την εφαρμογή, πρέπει να είστε εγγεγραμμένος χρήστης. Αυτό σημαίνει να δημιουργήσετε ένα προφίλ που αποκαλύπτει πληροφορίες για τον εαυτό σας. Μετά μπορείτε να κάνετε αναρτήσεις κειμένου, συμπεριλαμβανομένων φωτογραφιών και πολυμέσων, μπορείτε να τις μοιραστείτε με οποιονδήποτε άλλο χρήστη που έχει συμφωνήσει να γίνει «φίλος» σας. Το Facebook επιτρέπει την προσαρμογή διαφορετικών ρυθμίσεων απορρήτου, είτε το προφίλ σας είναι διαθέσιμο στο κοινό, είτε είναι διαθέσιμο μόνο προς το παρόν σε εσάς τους χρήστες. Η εφαρμογή επιτρέπει επίσης την επικοινωνία μεταξύ των χρηστών με το Facebook Messenger. Μπορείτε να διεξάγετε ιδιωτικές συνομιλίες, αλλά και να δημιουργήσετε ομαδικές ή να συμμετάσχετε σε αυτές ή ακόμα να συμμετέχετε σε ομάδες κοινού ενδιαφέροντος.
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο: **Απόρρητο,**	Το Facebook έχει συχνά επικριθεί για θέματα όπως η ιδιωτικότητα των χρηστών, η μαζική επιτήρηση, οι ψυχολογικές επιπτώσεις της πολιτικής χειραγώγησης, όπως ο εθισμός και η χαμηλή αυτοεκτίμηση, και περιεχόμενο όπως ψευδείς ειδήσεις, θεωρίες συνωμοσίας, παραβίαση πνευματικών δικαιωμάτων και ρητορική μίσους.

ακρίβεια, ιδιοκτησία, προσβασιμότητα, Παραβίαση νόμων, Πνευματικά δικαιώματα	***Απόρρητο:*** Στη σελίδα του FB μπορείτε να βρείτε τον άμεσο σύνδεσμο στους κανόνες απορρήτου: https://www.facebook.com/privacy/policy ***Ακρίβεια:*** https://www.facebook.com/policies_center/ads ***Ιδιοκτησία:*** Το Facebook θεωρεί καθήκον του να βοηθά τα άτομα και τους οργανισμούς να προστατεύουν τα δικαιώματα πνευματικής ιδιοκτησίας τους. Οι Όροι και Προϋποθέσεις του Facebook απαγορεύουν στους χρήστες να αναρτούν περιεχόμενο που παραβιάζει τα δικαιώματα πνευματικής ιδιοκτησίας άλλων, συμπεριλαμβανομένων των πνευματικών δικαιωμάτων και των δικαιωμάτων εμπορικών σημάτων. ***Πνευματικά δικαιώματα*** Τα πνευματικά δικαιώματα είναι θεσμοθετημένα δικαιώματα που προστατεύουν πρωτότυπα έργα δημιουργίας, όπως βιβλία, μουσικά έργα, ταινίες και έργα τέχνης, πρωτότυπες εκφράσεις, όπως δηλώσεις ή εικόνες. Δεν προστατεύουν γεγονότα ή ιδέες, αλλά μπορεί να προστατεύουν πρωτότυπες δηλώσεις ή εικόνες που περιγράφουν μια ιδέα. Τα πνευματικά δικαιώματα δεν προστατεύουν επίσης ονόματα, τίτλους ή σλόγκαν. Η προστασία τους παρέχεται από τους νόμους περί εμπορικών σημάτων. ***Εμπορικά σήματα*** Ένα εμπορικό σήμα είναι μια λέξη, ένα σύνθημα, ένα σύμβολο ή ένα σχέδιο (π.χ. ένα εμπορικό σήμα ή ένα λογότυπο) που διακρίνει τα προϊόντα και τις υπηρεσίες που προσφέρει μια οντότητα, ένας όμιλος ή μια εταιρεία από εκείνα που προσφέρουν άλλες οντότητες, όμιλοι ή εταιρείες. Η γενική λειτουργία της νομοθεσίας για τα εμπορικά σήματα είναι να βοηθά τους καταναλωτές να αναγνωρίζουν ποια οντότητα είναι υπεύθυνη για ένα συγκεκριμένο προϊόν ή υπηρεσία. https://www.facebook.com/help/399224883474207/?helpref=uf_share ***Προσβασιμότητα:*** Το Facebook παρέχει μια άνετη εμπειρία για όλους τους χρήστες. Διατίθενται λειτουργίες και τεχνολογίες που βοηθούν τα άτομα με αναπηρίες, όπως προβλήματα όρασης και ακοής, να χρησιμοποιούν το Facebook όσο το δυνατόν περισσότερο. ***Παραβίαση νόμων:*** Οι κρατικοί φορείς μπορεί να θεωρούν ότι το περιεχόμενο που δημοσιεύει ένας χρήστης στο Facebook παραβιάζει τους τοπικούς νόμους και μπορούν να ζητήσουν τον περιορισμό αυτού του περιεχομένου. Εάν δημοσιεύετε περιεχόμενο που δεν συμμορφώνεται με τους τοπικούς νόμους, ένα δικαστήριο μπορεί να διατάξει τον περιορισμό της δημοσίευσης του περιεχομένου ή να αναφέρει ισχυρισμούς ότι το περιεχόμενο είναι παράνομο, από μη κυβερνητικά ιδρύματα

	και μέλη του κοινού. Οι υποβολές εξετάζονται σύμφωνα με τις δεσμεύσεις της πρωτοβουλίας Global Network Initiative και τις εταιρικές αρχές για την προστασία των ανθρωπίνων δικαιωμάτων. https://transparency.fb.com/data/content-restrictions/content-violating-local-law/ ***Πνευματικά δικαιώματα:*** Οι νόμοι μπορεί να διαφέρουν από χώρα σε χώρα. Πληροφορίες για τα πνευματικά δικαιώματα είναι διαθέσιμες από το Γραφείο Πνευματικών Δικαιωμάτων των ΗΠΑ ή τον Παγκόσμιο Οργανισμό Πνευματικής Ιδιοκτησίας (WIPO). Το Facebook δεν παρέχει νομικές συμβουλές, οπότε συνιστάται να συμβουλευτείτε έναν δικηγόρο, εάν έχετε ερωτήσεις σχετικά με τα πνευματικά δικαιώματα. Στις περισσότερες χώρες, τα πνευματικά δικαιώματα είναι ένα θεσμοθετημένο δικαίωμα που προστατεύει τα πρωτότυπα έργα δημιουργίας. Συνήθως, ο δημιουργός ενός πρωτότυπου έργου αποκτά πνευματικά δικαιώματα επί του έργου αυτού κατά τη στιγμή της δημιουργίας του. Πολλοί διαφορετικοί τύποι περιεχομένου προστατεύονται από πνευματικά δικαιώματα, όπως: • *Οπτικό ή οπτικοακουστικό υλικό*: περιεχόμενο βίντεο, ταινίες, τηλεοπτικά προγράμματα και εκπομπές, βιντεοπαιχνίδια, πίνακες ζωγραφικής, φωτογραφίες • *Περιεχόμενο ήχου*: τραγούδια, μουσικές συνθέσεις, ηχογραφήσεις, ηχογραφήσεις προφορικών δηλώσεων • *Γραπτό περιεχόμενο*: βιβλία, θεατρικά έργα, χειρόγραφα, άρθρα, μουσικές σημειώσεις Τα πνευματικά δικαιώματα προστατεύουν μόνο τα πρωτότυπα έργα. Για να θεωρηθεί επαρκώς πρωτότυπο για την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας, το περιεχόμενο πρέπει να είναι έργο του δημιουργού και να έχει δημιουργηθεί με συγκεκριμένη ποσότητα δημιουργικής προσπάθειας.
Εμπόδια/δυσκολίες για ενήλικες	• Υψηλό επίπεδο αποκάλυψης ταυτότητας στο Facebook, όπως και σε άλλους ιστότοπους κοινωνικής δικτύωσης. Οι πληροφορίες που περιλαμβάνονται μπορεί να είναι όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου, φυσική διεύθυνση, αριθμός τηλεφώνου, φύλο, γενέτειρα, ημερομηνία γέννησης, φωτογραφία, δίκτυο φίλων, σεξουαλικός προσανατολισμός, κατάσταση σχέσης, ενδιαφέροντα, εργασία/επάγγελμα, αγαπημένα βιβλία, αγαπημένες ταινίες, αγαπημένη μουσική, σχολείο, πληροφορίες, ταχυδρομικός κώδικας και πολιτική τοποθέτηση. Οι προαναφερθείσες πληροφορίες είναι ιδιαίτερα ευαίσθητες, καθώς οι άνθρωποι αυτό-προσδιορίζονται αυθεντικά. • Η χρήση πραγματικών ονομάτων για την εκπροσώπηση ενός προφίλ μπορεί να ενθαρρύνεται μέσω τεχνικών προδιαγραφών, απαιτήσεων εγγραφής ή κοινωνικών κανόνων (σύνδεση των προφίλ των συμμετεχόντων με τις δημόσιες ταυτότητές τους). • Παρακολούθηση, επαναπροσδιορισμός ταυτότητας, δημογραφικός επαναπροσδιορισμός, επαναπροσδιορισμός προσώπου και κλοπή

	ταυτότητας. Οι χρήστες μπορεί να γίνουν θύματα κοινωνικής μηχανικής, παρενόχλησης, παρακολούθησης και spam. • Το Facebook μπορεί επίσης να προκαλέσει εθισμό. • Η διαδικτυακή επικοινωνία είναι πιο ελκυστική από την αλληλεπίδραση πρόσωπο με πρόσωπο. Αυτό μπορεί να δημιουργήσει ψυχαναγκαστική και υπερβολική χρήση των διαδικτυακών κοινωνικών δικτύων και να έχει δυσμενείς επιπτώσεις στα αποτελέσματα στην εργασία και στο σπίτι (αντισταθμίζοντας άλλες ελλείψεις όπως, σχέσεις, έλλειψη φίλων, σωματική εμφάνιση και αναπηρίες) • Καμία δυνατότητα καταγγελίας σεξουαλικών παραβατών στην αστυνομία, • Η αστυνομία εξέφρασε την ανησυχία της, επειδή το Facebook αποτυγχάνει να αντιμετωπίσει την απειλή των παιδόφιλων - δεν συμφώνησε να παρέχει ένα κουμπί πανικού στη σελίδα προφίλ κάθε χρήστη • Η αύξηση των εγκλημάτων όπως η παρενόχληση και η πραγματική σωματική βλάβη ως αποτέλεσμα της χρήσης του Facebook
Κίνδυνος μέσου/εργαλείου για τους ενήλικες	• Χάνετε τον έλεγχο του χρόνου που περνάτε στο διαδίκτυο. Η διάταξη των σελίδων, κάθε κουμπί, κάθε χρώμα είναι προσεκτικά επιλεγμένα από ειδικούς, για να προσελκύουν την προσοχή. • Ο αριθμός των ψεύτικων λογαριασμών στο Facebook είναι τεράστιος - τα λεγόμενα τρολ του διαδικτύου • Οι χάκερς γνωρίζουν πολύ καλά πώς να σπάσουν έναν κωδικό πρόσβασης στο FB. • Είναι πολύ συνηθισμένο να πλαστογραφούνται σελίδες σύνδεσης σε κοινωνικά δίκτυα και να αποστέλλονται ψευδή μηνύματα • Το Facebook χρησιμοποιείται συχνά ως εργαλείο για τη διάδοση ψευδών πληροφοριών • Οι πληροφορίες που δημοσιεύουμε εμείς οι ίδιοι στα μέσα κοινωνικής δικτύωσης μπορούν να χρησιμοποιηθούν από τρίτους. • Το Koobface ήταν ενεργό στο Facebook για πάνω από ένα χρόνο • Η κοινοποίηση της τοποθεσίας σας σε εφαρμογές και άλλους χρήστες μπορεί να έχει ως αποτέλεσμα την παρακολούθησή σας (π.χ. παρατήρηση του τόπου διαμονής σας, διάρρηξη). • Ο βιομετρικός έλεγχος ταυτότητας για πρόσβαση π.χ. στο κινητό σας τηλέφωνο ή σε διαδικτυακά προφίλ (με σάρωση προσώπου ή δακτυλικό αποτύπωμα) έχει επίσης αναδειχθεί ως απειλή.
Λύσεις που μπορούμε να έχουμε	Διαδικτυακή εκπαίδευση για το πώς να: • Χρησιμοποιείτε με ασφάλεια το Facebook, • Τι δεν πρέπει να δημοσιεύετε στα κοινωνικά δίκτυα (πώς να περιορίσετε την κοινοποίηση προσωπικών πληροφοριών για τον εαυτό σας) • Ρυθμίσεις απορρήτου στο FB. • Δημιουργήστε έναν ασφαλή κωδικό πρόσβασης για τον λογαριασμό σας • Ρύθμιση του ελέγχου ταυτότητας δύο παραγόντων. • Αποδοχή προσκλήσεων (αναγνώριση πρόσκλησης από ένα άτομο).

	• Διατήρηση ενημερωμένου λογισμικού προστασίας από ιούς και άλλου λογισμικού ασφαλείας. • Χρησιμοποιήστε την ενότητα Ιδιωτικές συνομιλίες. • Κοινή χρήση περιεχομένου, φωτογραφιών και αναρτήσεων από άλλα μέσα κοινωνικής δικτύωσης. • Πώς να αναφέρετε περιεχόμενο που φαίνεται ύποπτο.

Όνομα του μέσου κοινωνικής δικτύωσης/εργαλείου	**GOOGLE+**
Γενικές πληροφορίες	**Το Google+** ξεκίνησε στις 28 Ιουνίου 2011, σε μια προσπάθεια να αμφισβητήσει άλλα κοινωνικά δίκτυα, συνδέοντας άλλα προϊόντα της Google, όπως το Google Drive, το Blogger και το YouTube. Είναι συνήθως γνωστό ως Google Plus, μερικές φορές ονομάζεται G+. Είναι ένα κοινωνικό δίκτυο που ανήκει και λειτουργεί από την Google. Σημαντικές αλλαγές οδήγησαν σε επανασχεδιασμό αυτού του κοινωνικού δικτύου τον Νοέμβριο του 2015. Στις 7 Μαρτίου 2019 αποφασίστηκε να κλείσει το κοινωνικό δίκτυο για τις επιχειρήσεις και ένα μήνα αργότερα, στις 2 Απριλίου, έκλεισε και για τους προσωπικούς χρήστες. Ο λόγος αυτής της απόφασης ήταν τόσο η χαμηλή δέσμευση των χρηστών όσο και οι αποκαλυπτόμενες ατέλειες σχεδιασμού του λογισμικού που ενδεχομένως επέτρεπαν σε εξωτερικούς προγραμματιστές να έχουν πρόσβαση σε προσωπικές πληροφορίες των χρηστών του. Το Google+ συνέχισε να είναι διαθέσιμο ως "Google+ for G Suite".Όλοι οι χρήστες μεταπήδησαν στο "Google Currents". Το επόμενο βήμα θα είναι τελικά η μετάβαση από το Google Currents στο "Google Chat" το 2023. Στο Google+, οι άνθρωποι μπορούν να μοιράζονται ιδέες και προσωπικά νέα, να δημοσιεύουν φωτογραφίες και βίντεο, να μένουν σε επαφή, να παίζουν παιχνίδια, να προγραμματίζουν συναντήσεις, να στέλνουν ευχές για τα γενέθλιά τους, να κάνουν εργασίες και δουλειές μαζί, να βρίσκουν και να επικοινωνούν με χαμένους φίλους και συγγενείς, να αξιολογούν βιβλία, να προτείνουν εστιατόρια και να υποστηρίζουν σκοπούς. Ο κατάλογος συνεχίζεται - μπορείτε να δείτε πόσο ατομική είναι η χρήση του. Η κοινωνική δικτύωση περιλαμβάνει επίσης την απόκτηση και παροχή επικύρωσης και συναισθηματικής υποστήριξης, πολλή άτυπη μάθηση, καθώς και τη διερεύνηση προσωπικών, ακαδημαϊκών και μελλοντικών επαγγελματικών ενδιαφερόντων. Πρέπει να είστε εγγεγραμμένος χρήστης για να έχετε πλήρη πρόσβαση στις επιλογές του Google +. Κατά την είσοδο/εγγραφή θα σας ζητηθεί να απαντήσετε σε μερικές απλές ερωτήσεις, όπως το πραγματικό σας όνομα, ένα όνομα χρήστη, έναν κωδικό πρόσβασης και τα γενέθλιά σας. Στις Η.Π.Α. για να αποκτήσετε λογαριασμό, πρέπει να είστε τουλάχιστον 13 ετών, το ίδιο και σε άλλες χώρες. Θα σας δοθεί επίσης η δυνατότητα να προσθέσετε μια φωτογραφία προφίλ και στη συνέχεια θα μεταφερθείτε απευθείας στο Google+. Κατά τη διάρκεια της διαδικασίας εγγραφής θα σας ζητηθεί να

	«βρείτε άτομα που γνωρίζετε στο Google+», εισάγοντας μια διεύθυνση ηλεκτρονικού ταχυδρομείου από το Yahoo ή το Hotmail. Αυτό είναι προαιρετικό. Το Google+ δεν θα επικοινωνήσει με τα άτομα που βρίσκονται στη λίστα επαφών σας, αλλά θα εισάγει επαφές από αυτές τις υπηρεσίες και θα σας δώσει τη δυνατότητα να προσθέσετε τις επαφές σας από αυτές τις υπηρεσίες στους κύκλους σας. Μόλις αποκτήσετε λογαριασμό, την πρώτη φορά που θα επισκεφθείτε το Google+ θα σας ζητηθούν διάφορες ερωτήσεις, οι οποίες είναι προαιρετικές (όνομα σχολείου ή εργασίας και τόπος διαμονής για να διευκολύνετε τους φίλους, την οικογένεια και άλλους να σας βρουν).
Κίνδυνος που συνδέεται με το μέσο κοινωνικής δικτύωσης/ εργαλείο: **Ιδιωτικότητα, ακρίβεια, ιδιοκτησία, προσβασιμότητα, παραβίαση νόμων, πνευματικά δικαιώματα**	***Απόρρητο:*** Η ρύθμιση απορρήτου επέτρεπε στους χρήστες να αποκαλύπτουν ορισμένες πληροφορίες στους κύκλους της επιλογής τους. Οι χρήστες μπορούσαν επίσης να βλέπουν τους επισκέπτες του προφίλ τους. Υπήρχαν ρυθμίσεις απορρήτου, στις οποίες μπορούσατε να μεταβείτε κάνοντας κλικ στο όνομά σας στο επάνω δεξί μέρος της οθόνης σας και στη συνέχεια στην επιλογή Απόρρητο. Αυτό περιλάμβανε συνδέσμους για τη διαχείριση των κύκλων, την ορατότητα του δικτύου (ποιος ήταν στους κύκλους σας και ποιος μπορούσε να δει ποιος σας είχε προσθέσει στους κύκλους του) και άλλες ρυθμίσεις. Υπήρχε επίσης ένας σύνδεσμος προς την ενότητα βοήθειας για την ιδιωτικότητα του Google+. ***Ακρίβεια:*** Δεν υπάρχουν στοιχεία. ***Ιδιοκτησία:*** Ορισμένες εταιρείες διαχείρισης ιδιοκτησίας χρησιμοποίησαν το Google+ για να μοιραστούν τις δικές τους αναρτήσεις σε ιστολόγια, άρθρα τρίτων, νέα σχετικά με την επιχείρησή τους ή τον κλάδο γενικότερα κ.λπ. Το Google My Business έχει γίνει πλέον ο κεντρικός κόμβος όπου οι επισκέπτες του διαδικτύου μπορούν να βρουν και να μάθουν περισσότερα για την εταιρεία σας. ***Προσβασιμότητα:*** Τα περισσότερα από τα πράγματα που μπορείτε να κάνετε στο Google+ στον Ιστό μπορούν επίσης να γίνουν μέσω της εφαρμογής Google+ για έξυπνα τηλέφωνα για Android και iPhone, ενώ υπάρχει και μια εφαρμογή Ιστού που λειτουργεί με άλλα τηλέφωνα με σύνδεση στο Διαδίκτυο. Το Google Messenger είναι μια λειτουργία για έξυπνα τηλέφωνα (αλλά όχι για την έκδοση του Google+ για υπολογιστές) που επιτρέπει σε ομάδες ατόμων να συνομιλούν. ***Παραβίαση νόμων:*** Η Google εργάζεται σκληρά για να επιβάλει αυτούς τους κανόνες, αλλά με εκατομμύρια χρήστες και δισεκατομμύρια αναρτήσεις δεν μπορεί να τα κάνει όλα μόνη της. Σε αυτό το σημείο έρχεται η κοινότητα. Είναι στο χέρι όλων μας

	να διασφαλίσουμε ότι το Google+ θα παραμείνει ένα ασφαλές και άνετο μέρος. Αν δείτε περιεχόμενο που παραβιάζει τα πρότυπα, έχετε τη δυνατότητα να κάνετε κλικ στο κάτω βέλος στα δεξιά της δημοσίευσης ή του περιεχομένου και να επιλέξετε Αναφορά κατάχρησης. Στη συνέχεια, σας ζητείται να διευκρινίσετε γιατί είναι καταχρηστικό, τσεκάροντας το κατάλληλο πλαίσιο. Υπάρχει επίσης η επιλογή «Αναφορά αυτού του προφίλ» στην αριστερή στήλη του προφίλ κάθε ατόμου, εάν το ίδιο το προφίλ περιέχει περιεχόμενο που είναι πιθανό να παραβιάζει τα πρότυπα κοινότητας της Google. ***Πνευματικά δικαιώματα:*** Το βασικό σημείο αναφοράς για το ζήτημα της παραβίασης των πνευματικών δικαιωμάτων είναι οι Όροι χρήσης της Google. Η υπηρεσία της Google «Ανταποκρινόμαστε στις ειδοποιήσεις για εικαζόμενη παραβίαση πνευματικών δικαιωμάτων και τερματίζουμε τους λογαριασμούς των επαναλαμβανόμενων παραβατών σύμφωνα με τη διαδικασία που ορίζεται στον Νόμο Περί Πνευματικών Δικαιωμάτων της Ψηφιακής Χιλιετίας των ΗΠΑ. Παρέχουμε πληροφορίες για να βοηθήσουμε τους κατόχους πνευματικών δικαιωμάτων να διαχειριστούν την πνευματική τους ιδιοκτησία στο διαδίκτυο. Αν πιστεύετε ότι κάποιος παραβιάζει τα πνευματικά σας δικαιώματα και θέλετε να μας ειδοποιήσετε, μπορείτε να βρείτε πληροφορίες σχετικά με την υποβολή ειδοποιήσεων και την πολιτική της Google σχετικά με την απάντηση σε ειδοποιήσεις στο Κέντρο Βοήθειας».
Εμπόδια/δυσκολίες για ενήλικες	• Ο πιο συνηθισμένος κίνδυνος είναι η κοινωνική επιθετικότητα (διαδικτυακός εκφοβισμός) • Δημοσίευση ντροπιαστικών ή επιζήμιων πληροφοριών για τον εαυτό μας - κείμενα, φωτογραφίες ή βίντεο που θα μπορούσαν να μας φέρουν σε δύσκολη θέση τώρα ή αργότερα, είτε δημοσιεύονται από εμάς είτε από άλλους. Αυτό είναι το θέμα της φήμης/ κύρους. • Ο χρόνος μπροστά στην οθόνη - ο πολύς χρόνος που αφιερώνεται μπορεί να είναι επιζήμιος για άλλες δραστηριότητες στη ζωή μας. • Κίνδυνος ακατάλληλης επαφής με αγνώστους/χάκερ • Να είστε προσεκτικοί σχετικά με το ποιον προσκαλείτε σε ένα hangout και να συνειδητοποιήσετε ότι όποιος προσκαλείται μπορεί να προσκαλέσει και άλλα άτομα που μπορεί να μην γνωρίζετε.
Κίνδυνος μέσου/εργαλείου στους ενήλικες	Προς το παρόν η Google + δεν θα αποτελεί κίνδυνο για τους ενήλικες, καθώς το κοινωνικό δίκτυο έχει κλείσει από το 2019.
Λύσεις που μπορούμε να έχουμε	Εγχειρίδια ή οδηγοί που θα βοηθήσουν στη λήψη των δεδομένων που έχουν τεθεί στον λογαριασμό Google + που δημιουργήθηκε πριν από το 2019.

MILEAGE

Partners

E-Seniors (France) • www.eseniors.eu

CARDET (Cyprus) • www.cardet.org

EDUCATOR (Czech Republic) • www.educatorspolek.com

Framework (Italy) • www.aframework.it

WSBINOZ (Poland) • www.wsbinoz.edu.pl

Join us!

mileageproject info@mileageproject.eu www.mileageproject.eu

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. Project number: 2021-1-FR01-KA220-ADU-000033422