Co-funded by the European Union

Διαδικτυακές απειλές για άτομα άνω των 55 ετών - γλωσσάρι

Co-funded by the
European Union

Ηλεκτρονικό ψάρεμα (ψάρεμα μέσω ηλεκτρονικού ταχυδρομείου, SMS, σύνδεσμοι, φωνητικές κλήσεις)

Το ηλεκτρονικό ψάρεμα (phishing) είναι ένα είδος κυβερνοεπίθεσης όπου οι εγκληματίες στέλνουν ψεύτικα email, μηνύματα κειμένου, τηλεφωνικές κλήσεις ή συνδέσμους προσποιούμενοι ότι είναι κάποιος που εμπιστεύεστε, όπως μια τράπεζα ή ένας φίλος. Στόχος τους είναι να σας ξεγελάσουν ώστε να δώσετε σημαντικές προσωπικές πληροφορίες, όπως κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών ή στοιχεία τραπεζικού λογαριασμού. Αυτά τα ψεύτικα μηνύματα συχνά φαίνονται πολύ αληθινά και προσπαθούν να σας κάνουν να ενεργήσετε γρήγορα δημιουργώντας μια αίσθηση επείγοντος ή φόβου. Οι εισβολείς θέλουν να κλέψουν τα χρήματα ή την ταυτότητά σας ξεγελώντας σας ώστε να κάνετε κλικ σε επικίνδυνους συνδέσμους ή να κοινοποιήσετε ευαίσθητα δεδομένα. Για να παραμείνετε ασφαλείς, ελέγχετε πάντα ξανά ποιος έστειλε το μήνυμα, αποφεύγετε να κάνετε κλικ σε ύποπτους συνδέσμους και μην κοινοποιείτε ποτέ προσωπικές πληροφορίες εκτός εάν είστε απολύτως βέβαιοι ότι είναι ασφαλείς.

Co-funded by the
European Union

Deepfake επιθέσεις (ψεύτικος ήχος/βίντεο, πλαστοπροσωπία οικογένειας)

Οι επιθέσεις deepfake περιλαμβάνουν τη δημιουργία ψεύτικων ηχογραφήσεων ή βίντεο χρησιμοποιώντας τεχνητή νοημοσύνη που φαίνονται και ακούγονται πολύ αληθινές. Σε αυτές τις επιθέσεις, οι εγκληματίες μιμούνται τη φωνή ή το πρόσωπο κάποιου γνωστού, συχνά ενός μέλους της οικογένειας, για να ξεγελάσουν τους ανθρώπους ώστε να πιστέψουν ότι μιλάνε με ένα αγαπημένο τους πρόσωπο. Για παράδειγμα, ένας απατεώνας μπορεί να χρησιμοποιήσει τεχνολογία deepfake για να πραγματοποιήσει μια τηλεφωνική κλήση που ακούγεται ακριβώς σαν ένα εγγόνι που ζητάει επειγόντως χρήματα. Αυτές οι ψεύτικες ηχογραφήσεις είναι πολύ πειστικές και μπορούν να ξεγελάσουν ακόμη και προσεκτικούς ανθρώπους. Οι επιθέσεις deepfake είναι επικίνδυνες επειδή εκμεταλλεύονται την εμπιστοσύνη και τα συναισθήματα, καθιστώντας δύσκολη την συνειδητοποίηση της εξαπάτησης μέχρι να είναι πολύ αργά. Για να προστατεύσετε τον εαυτό σας, επαληθεύετε πάντα τα ασυνήθιστα αιτήματα επικοινωνώντας απευθείας με το άτομο μέσω διαφορετικών καναλιών επικοινωνίας πριν προβείτε σε οποιαδήποτε ενέργεια.

Co-funded by the
European Union

Ψεύτικα ηλεκτρονικά καταστήματα και απάτες (πλαστές ιστοσελίδες)

Τα ψεύτικα ηλεκτρονικά καταστήματα και οι απάτες είναι δόλιες ιστοσελίδες που έχουν σχεδιαστεί για να μοιάζουν με νόμιμα καταστήματα, αλλά στην πραγματικότητα δημιουργούνται για να ξεγελάσουν τους ανθρώπους ώστε να αγοράσουν προϊόντα που δεν υπάρχουν ή είναι κακής ποιότητας. Αυτά τα ψεύτικα καταστήματα συχνά αντιγράφουν λογότυπα, περιγραφές προϊόντων και φωτογραφίες από πραγματικές εταιρείες για να φαίνονται πειστικά. Οι απατεώνες χρησιμοποιούν αυτές τις ιστοσελίδες για να κλέψουν χρήματα και προσωπικά στοιχεία από ανυποψίαστους πελάτες. Δελεάζουν τους αγοραστές με υποσχέσεις για πολύ χαμηλές τιμές ή ειδικές προσφορές που φαίνονται πολύ καλές για να είναι αληθινές.

Αυτοί οι ιστότοποι ενδέχεται να έχουν παράξενες διευθύνσεις, ορθογραφικά λάθη ή να μην έχουν τα σωστά στοιχεία επικοινωνίας. Αφού οι πελάτες πληρώσουν, συχνά δεν λαμβάνουν ποτέ την παραγγελία τους ή λαμβάνουν πλαστά προϊόντα. Για να προστατεύσετε τον εαυτό σας, αγοράζετε πάντα από αξιόπιστα καταστήματα, ελέγχετε τις κριτικές των ιστότοπων, αποφεύγετε προσφορές που φαίνονται εξωπραγματικά φθηνές και μην κοινοποιείτε ποτέ στοιχεία πληρωμής σε ύποπτους ιστότοπους. Εάν κάτι σας φαίνεται περίεργο, είναι καλύτερο να το ελέγξετε ξανά πριν κάνετε μια αγορά.

Co-funded by the
European Union

Συναισθηματική χειραγώγηση και κοινωνική μηχανική (τακτικές εκφοβισμού)

Η συναισθηματική χειραγώγηση και η κοινωνική μηχανική περιλαμβάνουν την εξαπάτηση των ανθρώπων παίζοντας με τα συναισθήματά τους για να τους κάνουν να ενεργούν με τρόπους που κανονικά δεν θα ενεργούσαν. Οι κυβερνοεγκληματίες χρησιμοποιούν τακτικές όπως ιστορίες τρόμου, επείγον, ψεύτικη εξουσία ή καλοσύνη για να δημιουργήσουν ένα αίσθημα φόβου, εμπιστοσύνης ή υποχρέωσης. Για παράδειγμα, μπορεί να προσποιούνται ότι είναι τραπεζικός υπάλληλος που σας προειδοποιεί για ένα πρόβλημα με τον λογαριασμό σας, προτρέποντάς σας να ενεργήσετε γρήγορα, ώστε να παρέχετε ευαίσθητες πληροφορίες χωρίς να το σκεφτείτε. Αυτές οι τακτικές εκμεταλλεύονται τις φυσικές ανθρώπινες αντιδράσεις - φόβο, εμπιστοσύνη, περιέργεια ή βοήθεια - καθιστώντας δύσκολη την αντίσταση. Η καλύτερη άμυνα είναι η επίγνωση: αναγνωρίζοντας αυτά τα συναισθηματικά κόλπα και σταματώντας για να επαληθεύσετε ποιος πραγματικά ζητά πληροφορίες πριν απαντήσετε.

Co-funded by the
European Union

Κλοπή ταυτότητας (χρησιμοποιώντας κλεμμένα προσωπικά δεδομένα)

Κλοπή ταυτότητας σημαίνει όταν κάποιος κλέβει τα προσωπικά σας στοιχεία χωρίς την άδειά σας και τα χρησιμοποιεί για να προσποιηθεί ότι είστε εσείς. Μπορεί να χρησιμοποιήσει το όνομά σας, τον αριθμό κοινωνικής ασφάλισης, τα στοιχεία του τραπεζικού σας λογαριασμού ή άλλα δεδομένα για να ανοίξει λογαριασμούς, να λάβει δάνεια ή να κάνει αγορές στο όνομά σας. Αυτό μπορεί να προκαλέσει μεγάλα οικονομικά προβλήματα και να βλάψει τη φήμη σας.

Co-funded by the
European Union

Απάτη «στο εγγόνι» (απατεώνες που προσποιούνται ότι είναι οικογένεια σε κίνδυνο)

Η απάτη «στο εγγόνι», γνωστή και ως «απάτη με τον παππού και τη γιαγιά», είναι μια κοινή μέθοδος που χρησιμοποιείται από εγκληματίες που προσποιούνται ότι είναι μέλος της οικογένειας - συνήθως ένα εγγόνι ή ένα παιδί - που βρίσκεται σε κίνδυνο. Αυτό συμβαίνει συνήθως τηλεφωνικά, όπου ο απατεώνας καλεί ένα ηλικιωμένο άτομο και ισχυρίζεται ότι έχει σοβαρό πρόβλημα, όπως ατύχημα, σύλληψη ή ανάγκη επείγουσας οικονομικής βοήθειας. Ο καλών συχνά ζητά να σταλούν γρήγορα χρήματα και επιμένει να το κρατήσει μυστικό το θύμα, λέγοντας για παράδειγμα: «Μην το πεις στη μαμά, θα ανησυχήσει».

Αυτή η απάτη εκμεταλλεύεται συναισθήματα όπως η αγάπη και το ενδιαφέρον για τα μέλη της οικογένειας, κάνοντάς το άτομο να θέλει να βοηθήσει αμέσως χωρίς να σταματήσει να σκέφτεται. Όλο και περισσότερο, οι απατεώνες χρησιμοποιούν τεχνολογία όπως η τεχνητή νοημοσύνη για να μιμηθούν τη φωνή του πραγματικού εγγονιού, κάνοντας την κλήση να ακούγεται πολύ πειστική.

Co-funded by the
European Union

Ψεύτικα αιτήματα «βοήθειας» μέσω WhatsApp ή Messenger

Τα ψεύτικα αιτήματα «βοήθειας» μέσω WhatsApp ή Messenger είναι απάτες όπου κάποιος προσποιείται ότι είναι φίλος ή μέλος της οικογένειάς του που αντιμετωπίζει επείγοντα προβλήματα, ζητώντας χρήματα ή προσωπικά στοιχεία. Αυτά τα μηνύματα συχνά προέρχονται απροσδόκητα από άγνωστες ή συγκαλυμμένες επαφές. Ο απατεώνας μπορεί να πει ότι έχασε το τηλέφωνό του, ότι κλειδώθηκε έξω από τον λογαριασμό του ή ότι χρειάζεται επείγουσα οικονομική βοήθεια. Προσπαθούν να δημιουργήσουν μια αίσθηση επείγοντος και εμπιστοσύνης για να κάνουν τα θύματα να ενεργήσουν γρήγορα χωρίς να ελέγξουν αν είναι αλήθεια.

Co-funded by the
European Union

Ρομαντικές απάτες και απάτες που βασίζονται σε σχέσεις που χτίστηκαν στο διαδίκτυο

Οι απάτες με ρομαντικές σχέσεις είναι ένα είδος απάτης όπου οι εγκληματίες δημιουργούν ψεύτικα διαδικτυακά προφίλ και προσποιούνται ότι ενδιαφέρονται ρομαντικά για κάποιον. Χτίζουν εμπιστοσύνη και συναισθηματική σύνδεση με την πάροδο του χρόνου, κάνοντας το θύμα να πιστεύει ότι βρίσκεται σε μια γνήσια σχέση. Μόλις κερδίσουν την εμπιστοσύνη, οι απατεώνες επινοούν καταστάσεις έκτακτης ανάγκης ή επείγουσες οικονομικές ανάγκες - όπως ιατρικά έξοδα ή έξοδα ταξιδιού - και ζητούν από το θύμα χρήματα ή δώρα.

Αυτοί οι απατεώνες είναι πολύ επιδέξιοι στο να φαίνονται φροντιστικοί και αξιόπιστοι, αποφεύγοντας συχνά τις προσωπικές συναντήσεις ή τις βιντεοκλήσεις δίνοντας δικαιολογίες. Εκμεταλλεύονται τη μοναξιά και την συναισθηματική ευαλωτότητα, γεγονός που καθιστά τα θύματα πιο πιθανό να τους δώσουν χρήματα.

Co-funded by the
European Union

Επενδυτική απάτη (ψεύτικες διαφημίσεις με διασημότητες)

Η επενδυτική απάτη που περιλαμβάνει ψεύτικες διαφημίσεις με διασημότητες είναι ένα είδος απάτης όπου οι εγκληματίες χρησιμοποιούν εικόνες, βίντεο ή ονόματα διάσημων προσώπων για να κάνουν μια επενδυτική ευκαιρία να φαίνεται νόμιμη και αξιόπιστη. Μερικές φορές, αυτές οι διαφημίσεις περιλαμβάνουν deepfake βίντεο που δείχνουν διασημότητες να υποστηρίζουν μια επένδυση ή παρουσιάζονται ως ειδησεογραφικά άρθρα που συνδέουν διασημότητες με οικονομική επιτυχία με ορισμένες πλατφόρμες.

Οι απατεώνες ξεγελούν τους ανθρώπους κάνοντάς τους να πιστέψουν ότι μπορούν να αποκομίσουν γρήγορα και μεγάλα κέρδη, συχνά σε κρυπτονομίσματα ή συναλλαγές συναλλάγματος. Παρασύρουν τα θύματα να δημιουργήσουν λογαριασμούς, να καταθέσουν χρήματα και στη συνέχεια ζητούν περισσότερα χρήματα για να πληρώσουν ψεύτικες χρεώσεις ή φόρους. Οι πρόωρες επιστροφές μπορεί να αποδειχθούν ότι κερδίζουν την εμπιστοσύνη, αλλά όταν τα θύματα προσπαθούν να αποσύρουν τα χρήματά τους, μπλοκάρονται και τους ζητούνται μεγάλες πρόσθετες πληρωμές.

Co-funded by the
European Union

Κακόβουλο λογισμικό και ransomware (μολυσμένα αρχεία, συνημμένα)

Το κακόβουλο λογισμικό μπορεί να μολύνει τον υπολογιστή ή το τηλέφωνό σας και να προκαλέσει βλάβη, όπως κλοπή των προσωπικών σας στοιχείων, καταστροφή αρχείων ή κατάληψη του ελέγχου της συσκευής σας. Το ransomware είναι ένας ειδικός τύπος κακόβουλου λογισμικού που κλειδώνει ή κρυπτογραφεί τα αρχεία σας, καθιστώντας τα μη προσβάσιμα μέχρι να πληρώσετε λύτρα —συνήθως σε κρυπτονομίσματα— στον εισβολέα. Το ransomware μπορεί να εισέλθει στη συσκευή σας μέσω μολυσμένων συνημμένων email, κακόβουλων ιστότοπων ή μη ασφαλών λήψεων.

Μόλις μολυνθεί, το ransomware σάς εμποδίζει να χρησιμοποιήσετε τα σημαντικά αρχεία σας και μερικές φορές απαιτεί χρήματα για να αποκαταστήσετε την πρόσβαση. Η πληρωμή των λύτρων δεν εγγυάται ότι τα δεδομένα σας θα αποκαλυφθούν και ενθαρρύνει τους εγκληματίες να συνεχίσουν αυτές τις επιθέσεις.

Co-funded by the
European Union

Μη επαληθευμένες εφαρμογές και μη ασφαλείς λήψεις λογισμικού

Οι μη επαληθευμένες εφαρμογές και οι μη ασφαλείς λήψεις λογισμικού αποτελούν κυβερνοαπειλές όπου άτομα κατεβάζουν και εγκαθιστούν εφαρμογές ή αρχεία από άγνωστες ή αναξιόπιστες πηγές. Αυτές οι εφαρμογές ή οι λήψεις ενδέχεται να περιέχουν κρυφό κακόβουλο λογισμικό, ιούς ή spyware που μπορούν να βλάψουν τη συσκευή σας, να κλέψουν προσωπικά στοιχεία ή να δώσουν σε χάκερ μη εξουσιοδοτημένη πρόσβαση.

Επειδή αυτές οι εφαρμογές δεν ελέγχονται ή δεν εγκρίνονται από αξιόπιστες πλατφόρμες, μπορούν να επηρεάσουν την ασφάλεια της συσκευής σας, να προκαλέσουν σφάλματα ή να σας εκθέσουν σε απάτες. Οι ψεύτικες εφαρμογές μπορεί να μοιάζουν με πραγματικές, αλλά όταν εγκατασταθούν, μπορούν να συλλέξουν τα δεδομένα σας ή να διαδώσουν επιβλαβές λογισμικό.

Co-funded by the
European Union

Κοινοποίηση ευαίσθητων δεδομένων σε αγνώστους (φωτογραφίες, πληροφορίες)

Η κοινοποίηση ευαίσθητων δεδομένων σε αγνώστους, όπως φωτογραφίες ή προσωπικά στοιχεία, αποτελεί μια κυβερνοαπειλή όπου οι άνθρωποι αποκαλύπτουν προσωπικά στοιχεία σε άγνωστα ή μη έμπιστα άτομα στο διαδίκτυο. Αυτό μπορεί να φαίνεται ακίνδυνο, όπως η κοινοποίηση μιας φωτογραφίας, αλλά αυτά τα στοιχεία μπορούν να χρησιμοποιηθούν λανθασμένα για να κλέψουν την ταυτότητά σας, να διαπράξουν απάτη ή να βλάψουν τη φήμη σας.

Οι φωτογραφίες ενδέχεται να αποκαλύψουν το σπίτι, την τοποθεσία ή τις προσωπικές σας συνήθειες χωρίς να το συνειδητοποιείτε. Άγνωστοι μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να σας εξαπατήσουν ή να σας στοχοποιήσουν σε απάτες. Για να παραμείνετε ασφαλείς, κοινοποιήστε προσωπικές πληροφορίες και φωτογραφίες μόνο σε άτομα που εμπιστεύεστε, σκεφτείτε προσεκτικά πριν δημοσιεύσετε στο διαδίκτυο και προσαρμόστε τις ρυθμίσεις απορρήτου για να περιορίσετε ποιος μπορεί να δει τις πληροφορίες σας.

Co-funded by the
European Union

Διαρροές δεδομένων από τη χρήση παρωχημένων συσκευές ή λογισμικό

Η χρήση παρωχημένων συσκευών ή λογισμικού αποτελεί κυβερνοαπειλή, επειδή οι παλαιότερες εκδόσεις συχνά δεν διαθέτουν τις πιο πρόσφατες ενημερώσεις ασφαλείας. Αυτές οι ελλείπουσες ενημερώσεις δημιουργούν αδυναμίες, που ονομάζονται ευπάθειες, τις οποίες οι χάκερ μπορούν εύκολα να εκμεταλλευτούν για να αποκτήσουν πρόσβαση στα προσωπικά σας στοιχεία ή να ελέγξουν τη συσκευή σας. Αυτό μπορεί να οδηγήσει σε διαρροές δεδομένων, κλοπή ή μόλυνση από κακόβουλο λογισμικό.

Το παρωχημένο λογισμικό επιβραδύνει επίσης τη συσκευή σας και ενδέχεται να σταματήσει να λειτουργεί με νεότερα προγράμματα, δυσχεραίνοντας τις καθημερινές σας δραστηριότητες. Για να προστατευτείτε, είναι σημαντικό να ενημερώνετε τακτικά τη συσκευή και το λογισμικό σας με τις πιο πρόσφατες ενημερώσεις κώδικα και διορθώσεις ασφαλείας. Αυτό καλύπτει τα κενά ασφαλείας, διατηρεί τα δεδομένα σας ασφαλέστερα και διασφαλίζει την ομαλή λειτουργία της συσκευής σας.

Co-funded by the
European Union

Μαζικές εξατομικευμένες επιθέσεις με χρήση τεχνητής νοημοσύνης, στοχεύοντας προφίλ χρηστών

Οι μαζικά εξατομικευμένες επιθέσεις με χρήση τεχνητής νοημοσύνης είναι κυβερνοαπειλές όπου οι εισβολείς χρησιμοποιούν τεχνητή νοημοσύνη για να δημιουργήσουν εξαιρετικά προσαρμοσμένα και πειστικά μηνύματα που απευθύνονται σε άτομα με βάση τα προσωπικά τους δεδομένα. Η τεχνητή νοημοσύνη αναλύει πληροφορίες από μέσα κοινωνικής δικτύωσης, email και δημόσιες πηγές για να δημιουργήσει μηνύματα που φαίνονται πολύ οικεία και αξιόπιστα στον στόχο.

Αυτές οι επιθέσεις μπορούν να περιλαμβάνουν εξατομικευμένα email ή μηνύματα ηλεκτρονικού "ψαρέματος" (phishing) που αναφέρουν το όνομα, την εργασία, τις πρόσφατες δραστηριότητες ή τα ενδιαφέροντά του θύματος. Στόχος είναι να ξεγελαστούν οι άνθρωποι ώστε να κάνουν κλικ σε κακόβουλους συνδέσμους, να αποκαλύψουν κωδικούς πρόσβασης ή να μεταφέρουν χρήματα. Επειδή η Τεχνητή Νοημοσύνη μαθαίνει και προσαρμόζεται συνεχώς, αυτές οι επιθέσεις γίνονται πιο αποτελεσματικές και πιο δύσκολο να εντοπιστούν.

Co-funded by the
European Union

Παραπληροφόρηση για την υγεία ή επικίνδυνες ιατρικές συμβουλές από εργαλεία τεχνητής νοημοσύνης

Η παραπληροφόρηση για την υγεία ή οι επικίνδυνες ιατρικές συμβουλές από εργαλεία τεχνητής νοημοσύνης αποτελούν μια κυβερνοαπειλή όπου η τεχνητή νοημοσύνη παράγει λανθασμένες, παραπλανητικές ή επιβλαβείς πληροφορίες για την υγεία. Οι άνθρωποι μπορεί να εμπιστεύονται τα chatbots τεχνητής νοημοσύνης ή τα διαδικτυακά εργαλεία για ιατρικές συμβουλές, αλλά μερικές φορές αυτά τα συστήματα παράγουν λανθασμένες διαγνώσεις, προτείνουν μη ασφαλείς θεραπείες ή διαδίδουν ψευδείς ισχυρισμούς σχετικά με ασθένειες.

Αυτή η παραπληροφόρηση μπορεί να οδηγήσει τους ανθρώπους να καθυστερήσουν την κατάλληλη ιατρική περίθαλψη, να χρησιμοποιήσουν αναποτελεσματικά φάρμακα ή να προβούν σε επιβλαβείς ενέργειες. Το περιεχόμενο που δημιουργείται από την τεχνητή νοημοσύνη μπορεί να ακούγεται πολύ επαγγελματικό και πειστικό, καθιστώντας δύσκολο να διαπιστωθεί εάν οι συμβουλές είναι αξιόπιστες.

Co-funded by the
European Union

Απάτες που εκμεταλλεύονται τον ψηφιακό αποκλεισμό σε δημόσιες και τραπεζικές υπηρεσίες

Οι απάτες που εκμεταλλεύονται τον ψηφιακό αποκλεισμό στις δημόσιες και τραπεζικές υπηρεσίες αποτελούν απειλές που στοχεύουν άτομα που έχουν περιορισμένη πρόσβαση ή γνώση των ψηφιακών τεχνολογιών. Αυτές οι απάτες εκμεταλλεύονται άτομα που δυσκολεύονται να χρησιμοποιήσουν διαδικτυακές κυβερνητικές ή τραπεζικές υπηρεσίες, μερικές φορές επειδή δεν έχουν συσκευές, πρόσβαση στο διαδίκτυο, ψηφιακές δεξιότητες ή αυτοπεποίθηση.

Οι εγκληματίες ξεγελούν αυτά τα άτομα προσφέροντας ψεύτικη βοήθεια με διαδικτυακές διαδικασίες ή στέλνοντας δόλια μηνύματα που μιμούνται επίσημα ιδρύματα, ελπίζοντας ότι τα θύματα θα κοινοποιήσουν ευαίσθητα δεδομένα ή θα στείλουν χρήματα. Επειδή αυτά τα άτομα έχουν λιγότερους πόρους ή υποστήριξη για να αναγνωρίσουν απάτες, είναι πιο ευάλωτα.

Co-funded by the European Union

Έλλειψη πρακτικών πολυπαραγοντικής επαλήθευσης ταυτότητας (απλοποιημένοι κωδικοί πρόσβασης, επαναχρησιμοποίηση)

Η έλλειψη πολυπαραγοντικού ελέγχου ταυτότητας (MFA) σημαίνει ότι χρησιμοποιείτε μόνο έναν κωδικό πρόσβασης —συχνά απλό ή επαναλαμβανόμενο σε πολλούς ιστότοπους— για την προστασία των διαδικτυακών λογαριασμών. Αυτό είναι επικίνδυνο, επειδή αν κάποιος κλέψει ή μαντέψει τον κωδικό πρόσβασής σας, μπορεί εύκολα να αποκτήσει πρόσβαση στους λογαριασμούς σας.

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων προσθέτει ένα επιπλέον επίπεδο ασφάλειας, απαιτώντας δύο ή περισσότερες μορφές επαλήθευσης. Για παράδειγμα, αφού πληκτρολογήσετε τον κωδικό πρόσβασής σας, ενδέχεται να εισαγάγετε έναν κωδικό που αποστέλλεται στο τηλέφωνό σας ή να χρησιμοποιήσετε σάρωση δακτυλικών αποτυπωμάτων. Αυτό καθιστά πολύ πιο δύσκολο για τους χάκερ να αποκτήσουν πρόσβαση στον λογαριασμό σας, ακόμα κι αν έχουν τον κωδικό πρόσβασής σας.

Co-funded by the
European Union

Απώλεια πρόσβασης σε κρίσιμες υπηρεσίες λόγω τεχνολογικών αλλαγών (πρόσβαση μόνο μέσω εφαρμογής, περιορισμένες εναλλακτικές λύσεις)

Η απώλεια πρόσβασης σε κρίσιμες υπηρεσίες λόγω τεχνολογικών αλλαγών συμβαίνει όταν σημαντικές δημόσιες ή τραπεζικές υπηρεσίες μεταβαίνουν σε αποκλειστικά ψηφιακές μορφές, όπως εφαρμογές ή διαδικτυακές πύλες, χωρίς εύκολες εναλλακτικές λύσεις για άτομα που δεν είναι άνετα ή δεν είναι εξοπλισμένα για να τις χρησιμοποιήσουν. Αυτό σημαίνει ότι άτομα που δεν διαθέτουν smartphone, υπολογιστές ή ψηφιακές δεξιότητες μπορεί να δυσκολεύονται ή να μην έχουν πρόσβαση σε βασικές υπηρεσίες, όπως ραντεβού υγειονομικής περίθαλψης, συνταξιοδοτικά επιδόματα ή τραπεζικές συναλλαγές.

Αυτή η ψηφιακή μετάβαση μπορεί να αποκλείσει πολλούς, ειδικά ηλικιωμένους ενήλικες ή άτομα με περιορισμένους πόρους, καθιστώντας τους εξαρτημένους από άλλους ή ανίκανους να ολοκληρώσουν σημαντικές εργασίες.

Co-funded by the
European Union

Αυτοματοποιημένη χειραγώγηση των ροών των μέσων κοινωνικής δικτύωσης, παραγωγή παραπληροφόρησης και άγχους

Η αυτοματοποιημένη χειραγώγηση των ροών κοινωνικής δικτύωσης αποτελεί μια κυβερνοαπειλή όπου προγράμματα υπολογιστών, που ονομάζονται bots, και η τεχνητή νοημοσύνη ελέγχουν το περιεχόμενο που βλέπετε στις σελίδες σας στα μέσα κοινωνικής δικτύωσης. Αυτά τα συστήματα αναλύουν τι σας αρέσει, τι κοινοποιείτε ή τι σχολιάζετε και, στη συνέχεια, σας εμφανίζουν περισσότερες παρόμοιες αναρτήσεις για να σας κρατήσουν αφοσιωμένους.

Δυστυχώς, αυτό μπορεί να χρησιμοποιηθεί για τη διάδοση παραπληροφόρησης, ψευδών ειδήσεων ή ακραίου περιεχομένου που προκαλεί άγχος, φόβο ή θυμό. Τα bots μπορούν να ενισχύσουν τεχνητά τη δημοτικότητα τέτοιων αναρτήσεων επισημαίνοντας με like, κοινοποιώντας ή σχολιάζοντας, κάνοντάς τους να φαίνονται ότι πολλοί άνθρωποι συμφωνούν μαζί τους.