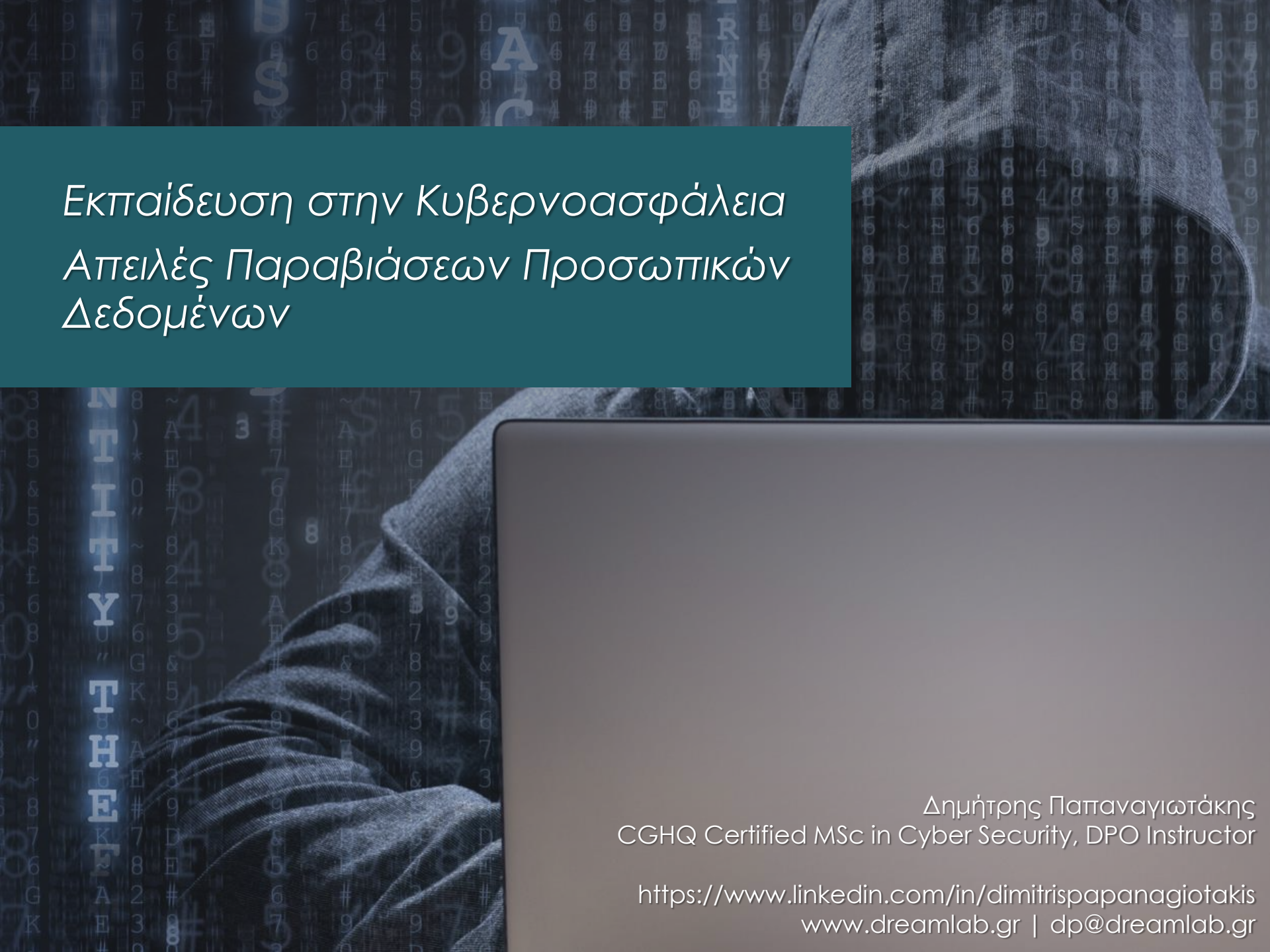


Εκπαίδευση στην Κυβερνοασφάλεια

Απειλές Παραβιάσεων Προσωπικών Δεδομένων

Δημήτρης Παπαναγιωτάκης
CGHQ Certified MSc in Cyber Security, DPO Instructor

https://www.linkedin.com/in/dimitrispapanagiotakis
www.dreamlab.gr | dp@dreamlab.gr

Η Κλοπή Ταυτότητας (Identity Theft) είναι πρόβλημα όλων μας

Η κλοπή ταυτότητας είναι το ταχύτερα αναπτυσσόμενο έγκλημα στις ΗΠΑ

Source: Trans Union Website, January 14, 2015

Κάθε 2-3 δευτερόλεπτα «κλέβεται» η ταυτότητα ενός υποκειμένου.

Source: https://identity.utexas.edu/id-perspectives/top-10-myths-about-identity-theft

Το μέσο κόστος ανά κλοπή ταυτότητας υπολογίζεται στα $4,930.

Source: U.S. Department of Justice, Javelin Strategy & Research

Κατά μέσο όρο, χρειάζονται 600 ώρες για πλήρη ανάκαμψη από κλοπή ταυτότητας.

Source: The Identity Theft Resource Center website, April 28, 2015

Το θέμα δεν είναι ΑΝ αλλά πότε…

13.1 εκατ.
υποκείμενα έπεσαν θύματα κλοπής ταυτότητας το 2015.

Source: Javelin 2016 Identity Fraud Study

63%
των επιβεβαιωμένων παραβιάσεων δεδομένων αφορούσε αδύναμους, προεπιλεγμένους ή κλεμμένους κωδικούς πρόσβασης.

Source: Verizon 2016 Data Breach Investigations Report

Σε άνω του **95%**
του συνόλου των περιστατικών ασφαλείας που διερευνήθηκαν το «ανθρώπινο σφάλμα» αναγνωρίστηκε ως παράγοντας που έπαιξε καταλυτικό ρόλο.

Source: IBM Security Services 2014 Cyber Security Intelligence Index

Θέματα Εκπαίδευσης

- Αναγνώριση κοινών κυβερνοαπειλών - cyberthreats
- Πως οι εγκληματίες του κυβερνοχώρου (black hat hackers) χρησιμοποιούν κλεμμένα δεδομένα
- Μελέτες περιπτώσεων
- Προστατέψτε τα δεδομένα του υποκειμένου
- Βέλτιστες πρακτικές για την προστασία των δεδομένων υποκειμένων
- Μύθοι και αλήθειες
- Ανταπόκριση σε παραβίαση δεδομένων
- Πόροι

Αναγνώριση κοινών κυβερνοαπειλών - cyberthreats

Συχνότερες Κυβερνοαπειλές

1. Email Account Takeover
2. Malware
3. Phishing
4. Credential Replay
5. Social Engineering
6. Call Forwarding
7. Spoofing

Email Account Takeover
Κατάληψη Λογαριασμού Email

Τι είναι;
Ένας κυβερνοεγκληματίας «χακάρει» ένα λογαριασμό email και ψάχνει το mailbox για αλληλογραφία που αφορά οικονομικές συναλλαγές μεταξύ πελατών προμηθευτών ή με χρηματοπιστωτικά ιδρύματα. Στόχος είναι να παρακολουθήσουν τη συμπεριφορά του θύματος και την κατάλληλη στιγμή να αποκομίσει οικονομικό όφελος.

Πως το αντιλαμβάνεστε;
Υπάρχει αλληλογραφία η οποία αφορά αίτημα μεταφοράς κεφαλαίων σε κάποιο λογαριασμό. Ο κυβερνοεγκληματίας υποδύεται τον πελάτη προς τα χρηματοπιστωτικά ιδρύματα ή τον προμηθευτή του και επικοινωνεί με το θύμα. Σε κάθε περίπτωση προσπαθεί να αποκομίσει οικονομικό όφελος κλέβοντας χρήματα του πελάτη.

Πως συμβαίνει;
Οι κυβερνοεγκληματίες εντοπίζουν και εκμεταλλεύονται ευπάθειες στους διακομιστές των παρόχων (Yahoo, Hotmail, ISPs) υπηρεσιών ή στις διευθύνσεις IP των Η/Υ των χρηστών για να αποκτήσουν πρόσβαση σε διαπιστευτήρια σύνδεσης ή απευθείας στον λογαριασμό ηλεκτρονικού ταχυδρομείου.

Ποιες είναι οι επιπτώσεις;
Επειδή ο κυβερνοεγκληματίας έχει πρόσβαση στο email του πελάτη μας και μπορεί να τον μιμηθεί, είναι πιθανό ο παραλήπτης να πειστεί ότι η αλληλογραφία προέρχεται από τον πελάτη. Οι εγκληματίες του κυβερνοχώρου ενδέχεται να στείλουν οδηγίες για τη μεταφορά χρημάτων σε δικό τους λογαριασμό. Χωρίς σωστή επαλήθευση, τα χρήματα θα μπορούσαν να μεταφερθούν και να κλαπούν. Σε περίπτωση που ο λογαριασμός email είναι εταιρικός η επιχείρηση μπορεί να θεωρηθεί υπεύθυνη για τυχών οικονομική βλάβη πελατών.

Πως μπορείτε να αμυνθείτε;
- Μην ενεργείτε με αιτήματα που προέρχονται από το ηλεκτρονικό ταχυδρομείο όταν αφορούν ευαίσθητες πληροφορίες, κινήσεις χρημάτων ή συναλλαγές. Προβείτε σε επαλήθευση όλων των αιτημάτων με τους πελάτες και αποστολή ερωτήσεων.
- Ακολουθήστε τις κατάλληλες διαδικασίες αναγνώρισης / επαλήθευσης. Χρησιμοποιήστε μυστικούς κωδικούς πρόσβασης, επαληθεύσεις τηλεφωνικών κλήσεων και ή κάντε βιντεοκλήση για να επιβεβαιώσετε την ταυτότητα του πελάτη.

Malware – Κακόβουλο Λογισμικό

Πως λειτουργεί;
Το κακόβουλο λογισμικό δημιουργείται για να καταστρέψει / απενεργοποιήσει τους υπολογιστές και τα συστήματα υπολογιστών, να κλέψει δεδομένα ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στα δίκτυα.

Πως το αντιλαμβάνεστε;
Παραδείγματα κακόβουλου λογισμικού είναι οι ιοί, τα worms, τα Trojan horses, τα ransomware, και τα spyware.

Πως συμβαίνει;
Το κακόβουλο λογισμικό μπορεί να εγκατασταθεί σε έναν υπολογιστή όταν ένας χρήστης κάνει κλικ σε έναν μη ασφαλές σύνδεσμο, ανοίγει ένα μολυσμένο αρχείο ή επισκέπτεται έναν αξιόπιστο ιστότοπο που θα μπορούσε να περιέχει adware.

Ποιες είναι οι επιπτώσεις;
Το κακόβουλο λογισμικό μπορεί να διαγράψει αρχεία ή πληροφορίες καταλόγου ή μπορεί να επιτρέψει στους επιτιθέμενους να συλλέγουν συγκεκαλυμμένα προσωπικά δεδομένα, συμπεριλαμβανομένων των οικονομικών πληροφοριών και των ονομάτων χρηστών και κωδικών πρόσβασης.

Πως μπορείτε να αμυνθείτε;
- Μην κάνετε κλικ σε ύποπτους συνδέσμους
- Μην ανοίγετε επισυνάψεις ή συνδέσμους που περιλαμβάνονται σε ανεπιθύμητα email ακόμη και αν γνωρίζεται τον αποστολέα.
- Μην ανοίγετε ή μεταφορτώνετε προγράμματα, λογισμικό, αρχεία κ.λπ. χωρίς προηγούμενο έλεγχο/έγκριση από εξουσιοδοτημένο προσωπικό.
- Μην εισάγετε κανένα USB που λάβατε από άγνωστη / αναξιόπιστη πηγή.

Phishing

70% των κυβερνοεπιθέσεων είναι αποτέλεσμα phishing και hacking

Source: Verizon 2015 Data Breach Investigations Report

Τι είναι;
Οι κυβερνοεγκληματίες προσποιούνται ότι είναι μια αξιόπιστη πηγή προκειμένου να αποκτήσουν ευαίσθητα προσωπικά στοιχεία όπως ονόματα χρήστη, κωδικούς πρόσβασης, αριθμούς κοινωνικής ασφάλισης και στοιχεία πιστωτικών καρτών.

Πως το αντιλαμβάνεστε;
Ένα μήνυμα ηλεκτρονικού ταχυδρομείου, μια τηλεφωνική κλήση ή ένα μήνυμα κειμένου από φαινομενικά νόμιμη διεύθυνση ή αριθμό ηλεκτρονικού ταχυδρομείου σας δίνει οδηγίες να κάνετε κλικ σε ένα σύνδεσμο για να αναλάβετε δράση (π.χ. «επικαιροποιήστε τον λογαριασμό σας», «επιβεβαιώστε την ταυτότητά σας» και «διεκδικήστε το δώρο σας»). Ο σύνδεσμος σάς φέρνει σε έναν ιστότοπο που σας ζητά να καταχωρίσετε τα προσωπικά σας στοιχεία.

Πως συμβαίνει;
Επειδή ο κυβερνοεγκληματίας μεταμφιέζετε σε νόμιμη πηγή (π.χ. υπάλληλος χρηματοπιστωτικών ιδρυμάτων, πελάτης, τραπεζίτης, κρατική αρχή), σας πείθει ότι το αίτημα προέρχεται από αξιόπιστη πηγή και υποχρεώνεστε άθελά σας να δώσετε προσωπικά δεδομένα όταν σας τα ζητούν.

Ποιες είναι οι επιπτώσεις;
Τα θύματα ηλεκτρονικού «ψαρέματος» ενδέχεται να έχουν εγκατεστημένο κακόβουλο λογισμικό στα συστήματα ηλεκτρονικών υπολογιστών τους ή να έχουν πέσει θύματα κλοπής της ταυτότητά τους.

Πως μπορείτε να αμυνθείτε;
- Τοποθετήστε το δείκτη του ποντικιού πάνω από αμφισβητούμενους συνδέσμους για να αποκαλύψετε τον πραγματικό προορισμό πριν κάνετε κλικ.
- Προσοχή στις κλωνοποιημένες ιστοσελίδες που μπορεί να φαίνονται νόμιμες. Σημειώστε ότι οι ασφαλείς ιστότοποι ξεκινούν με https, όχι http.
- Ειδοποιήστε τον υπεύθυνο ασφαλείας και τον αποστολέα αμέσως μόλις λάβετε ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου.

Credential Replay – Επανάληψη Διαπιστευτηρίων

Τι είναι;
Οι περισσότεροι χρήστες επαναχρησιμοποιούν κωδικούς πρόσβασης και ονόματα χρηστών (γνωστά και ως «διαπιστευτήρια»). Οι κυβερνοεγκληματίες αποκτούν αυτά τα διαπιστευτήρια σύνδεσης, τα δοκιμάζουν σε μεγάλο αριθμό ιστοτόπων όπως χρηματοπιστωτικά ιδρύματα, webmail συστήματα ώστε να αποκτήσουν πρόσβαση και, στη συνέχεια, αιτούνται δόλιες μεταφορές κεφαλαίων. Εναλλακτικά, μπορούν να μεταπωλούν αυτές τις πληροφορίες σε άλλους κυβερνοεγκληματίες για να αποκτήσουν κέρδος. Αυτοί οι κυβερνοεγκληματίες μπορούν στη συνέχεια να χρησιμοποιήσουν αυτές τις πληροφορίες για να διαπράξουν απάτη.

Πως το αντιλαμβάνεστε;
Οι κυβερνοεγκληματίες ελπίζουν να έχουν πρόσβαση σε μερικούς λογαριασμούς χρησιμοποιώντας μια μεγάλη μνήμη κλεμμένων διαπιστευτηρίων σύνδεσης για να αποκτήσουν πρόσβαση σε ηλεκτρονικούς λογαριασμούς ατόμων και επιχειρήσεων.

Πως συμβαίνει;
Εάν οι εγκληματίες του κυβερνοχώρου δεν κλέβουν τα ίδια αυτά τα διαπιστευτήρια, μπορούν εύκολα να αγοράσουν μεγάλο αριθμό κλεμμένων διαπιστευτηρίων σύνδεσης από το dark web. Αυτές οι μεγάλες ποσότητες διαπιστευτηρίων προέρχονται συνήθως από παραβιάσεις δεδομένων (π.χ. Yahoo, Verizon, LinkedIn, κλπ.).

Ποιες είναι οι επιπτώσεις;
Ο λογαριασμός σας παραβιάζεται, και οι κυβερνοεγκληματίες μπορούν γρήγορα να επαναχρησιμοποιήσουν τα διαπιστευτήρια για να δοκιμάσουν να αποκτήσουν πρόσβαση και σε άλλους λογαριασμούς με άμεσο αποτέλεσμα οικονομική βλάβη αλλά και κλοπή προσωπικών δεδομένων πριν εντοπιστούν.

Πως μπορείτε να αμυνθείτε;
- Να χρησιμοποιήσετε έναν μοναδικό κωδικό πρόσβασης για κάθε λογαριασμό για να αποτρέψετε μια γρήγορη και επεμβατική επίθεση σε όλους τους λογαριασμούς σας.
- Κάντε κάθε κωδικό πρόσβασης μοναδικό και μακρύ και ισχυρό. Χρησιμοποιήστε τουλάχιστον 8-12 χαρακτήρες, κεφαλαία γράμματα και σύμβολα.
- Χρησιμοποιήστε μεθόδους ελέγχου ταυτότητας διπλού παράγοντα (π.χ. SMS ή tokens)

Social Engineering – Κοινωνική Μηχανική

Τι είναι;
Η μέθοδος λειτουργεί με την ψυχολογική χειραγώγηση των ανθρώπων, προκειμένου να δημιουργηθεί ένα επίπεδο εμπιστοσύνης που οδηγεί στην ατομική ανάληψη δράσης (π.χ. αποκάλυψη ευαίσθητων και ιδιωτικών πληροφοριών, έναρξη αίτησης εκταμίευσης κεφαλαίων κ.λπ.). Η πιο συνηθισμένη μορφή είναι "phishing". Σε αυτό το σενάριο, τα διαπιστευτήρια των πελατών μας αποκτώνται από εξωτερικές πηγές (δηλ. το darkweb).

Πως το αντιλαμβάνεστε;
Μια κυβερνοεγκληματίας γίνεται φίλος με τον χρήστη στόχο με σκοπό να χτίζει εμπιστοσύνη του με την πάροδο του χρόνου, μέχρι να είναι σε θέση να ζητήσει ευαίσθητες πληροφορίες από τον στόχο. Οι πληροφορίες αυτές μπορούν στη συνέχεια να χρησιμοποιηθούν για τη διάπραξη απάτης.

Πως συμβαίνει;
Συχνά οι εγκληματίες στον κυβερνοχώρο επικοινωνούν με τα θύματα μέσω τηλεφώνου, ηλεκτρονικού ταχυδρομείου ή μέσω κοινωνικών μέσων.

Ποιες είναι οι επιπτώσεις;
Ο εγκληματίας διαπράττει απάτη, κλέβει τα χρήματα του πελάτη μας ή ευαίσθητες πληροφορίες και στη συνέχεια εξαφανίζεται.

Πως μπορείτε να αμυνθείτε;
- Εκπαιδεύστε τους χρήστες σας σχετικά με τις πληροφορίες που επιλέγουν να μοιραστούν στα κοινωνικά μέσα δικτύωσης, διατηρώντας τις προσωπικές τους πληροφορίες ιδιωτικές (όπως διεύθυνση κατοικίας, αριθμός τηλεφώνου, εργοδότης, ημερομηνίες διακοπών και ημερομηνία γέννησης).
- Επιβεβαιώστε την πηγή του αιτήματος.

Call Forwarding – Εκτροπή Κλήσεων

Τι είναι;
Ο κυβερνοεγκληματίας έχει καταφέρει, είτε μέσω τηλεφωνικής εταιρείας, είτε έχοντας χακάρει το τηλεφωνικό κέντρο ή μια μεμονωμένη συσκευή να εκτρέπει όλες τις κλήσεις προς τον αριθμό του θύματος στο δικό του τηλέφωνό.

Πως το αντιλαμβάνεστε;
Ο κυβερνοεγκληματίας καλεί την τηλεφωνική εταιρεία και υποδύεται πως είναι ο πελάτης εκτελώντας την τυπική διαδικασία ταυτοποίησης. Στη συνέχεια αιτείται ενεργοποίησης άμεσης εκτροπής όλων των κλήσεων σε αριθμό της επιλογής του. Στη συνέχεια επικοινωνεί με χρηματοπιστωτικό ίδρυμα και ζητά να τον καλέσουν πίσω (τυπική διαδικασία ταυτοποίησης) πριν προχωρήσει σε αιτήματα μεταφοράς χρημάτων (έχει ήδη το PIN του θύματος για το phone banking).

Πως συμβαίνει;
Οι κυβερνοεγκληματίες εξαπατούν την τηλεφωνική εταιρεία ενεργοποιώντας εκτροπή ή ο στόχος κάνει κλικ σε κάποιο link και που οδηγεί σε κακόβουλο λογισμικό μολύνοντας το «έξυπνο κινητό του».

Ποιες είναι οι επιπτώσεις;
Το τηλέφωνο σας έχει παραβιαστεί, οι συνομιλίες σας μπορεί να υποκλαπούν, η ταυτότητα σας έχει κλαπεί. Υπάρχει σοβαρή πιθανότητα οικονομικής βλάβης.

Πως μπορείτε να αμυνθείτε;
- Ακολουθήστε τις κατάλληλες διαδικασίες επαλήθευσης ταυτότητας Σκεφτείτε να χρησιμοποιήσετε μυστικούς κωδικούς πρόσβασης για να επιβεβαιώσετε την ταυτότητα των ατόμων με τα οποία επικοινωνείτε.
- Εκπαίδευση των χρηστών ώστε να ελέγχουν και να ταυτοποιούν την πηγή των κλήσεων που δέχονται.

Spoofing - Πλαστογράφηση

Τι είναι;
Κάλυψη της πηγής μιας επικοινωνίας (τηλέφωνο ή ηλεκτρονικό ταχυδρομείο) για να μοιάζει με μια αξιόπιστη πηγή (π.χ., κυβέρνηση, κλήση μέσα σε μια εταιρεία, κ.λπ.).

Πως το αντιλαμβάνεστε;
Λαμβάνουμε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από έναν κυβερνοεγκληματία που υποδύεται έναν από τους πελάτες μας και επιβεβαιώνει μια δόλια αίτηση μεταφοράς χρημάτων.

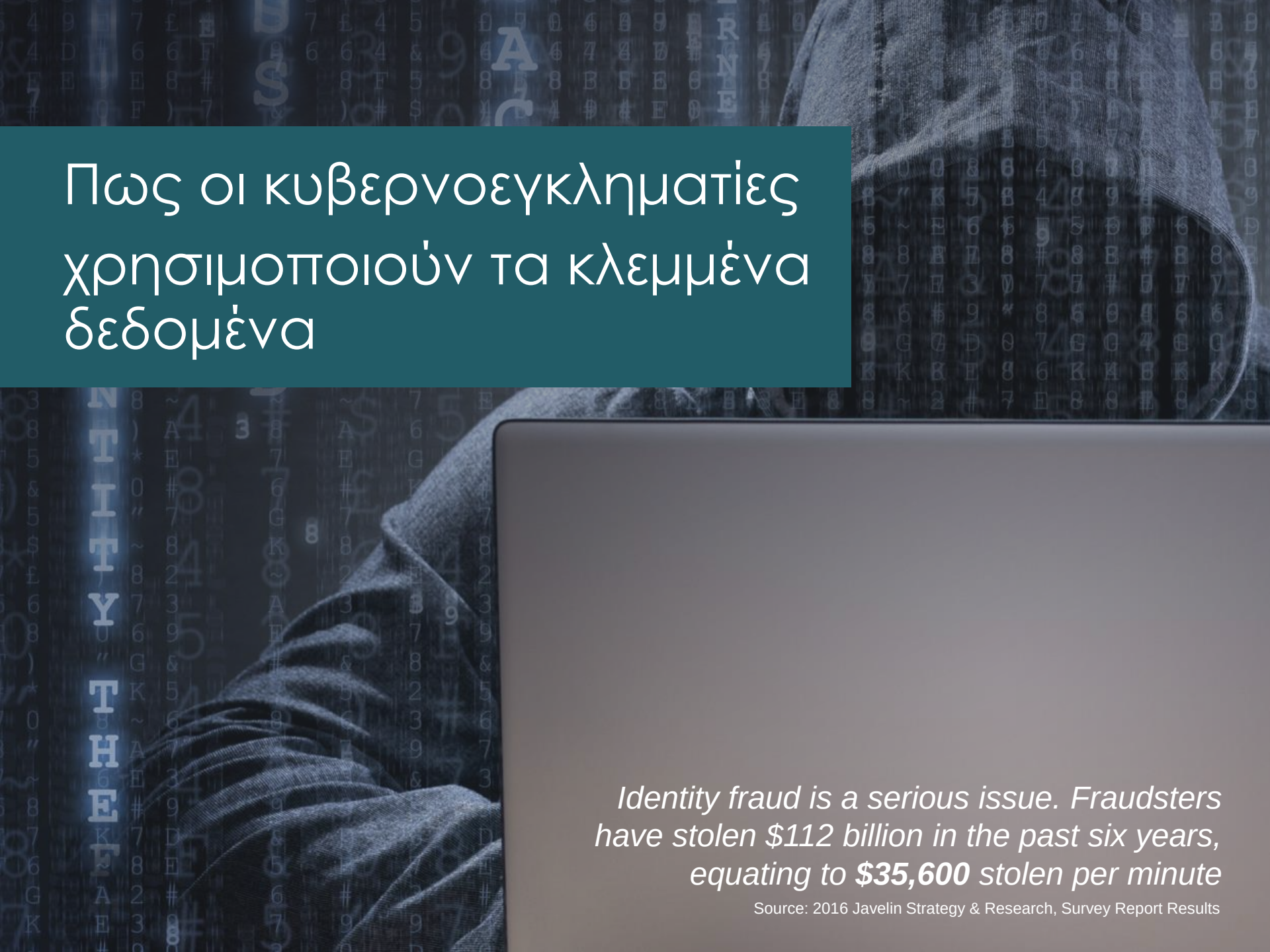
Πως συμβαίνει;
Υπάρχουν εύκολα εργαλεία διαθέσιμα στους κυβερνοεγκληματίες που βοηθούν στην κάλυψη της πηγής / αποστολέα. Για παράδειγμα, ο εγκληματίας του κυβερνοχώρου μπορεί να δημιουργήσει μια διεύθυνση ηλεκτρονικού ταχυδρομείου σχεδόν ταυτόσημη με τη διεύθυνση ηλεκτρονικού ταχυδρομείου του πελάτη (δηλ., Απενεργοποιημένη από έναν χαρακτήρα), έτσι ώστε η διεύθυνση ηλεκτρονικού ταχυδρομείου να εμφανίζεται αξιόπιστη.

Οι εγκληματίες του κυβερνοχώρου βασίζονται στην έλλειψη προσοχής μας στη λεπτομέρεια για να διαπράξουν την απάτη.

Ποιες είναι οι επιπτώσεις;
Παρόμοια με τους άλλους τύπους κυβερνοεπιθέσεων που έχουμε συζητήσει, τα χρήματα του πελάτη μας αποτελούν στόχο, γίνονται θύματα απάτης ή / και κλοπής ταυτότητας.

Πως μπορείτε να αμυνθείτε;
- Ελέγξτε προσεκτικά τα εισερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου για τη σωστή διεύθυνση ηλεκτρονικού ταχυδρομείου και την ακρίβεια της ορθογραφίας του ονόματος του αποστολέα. Τοποθετήστε το δείκτη του ποντικιού πάνω από το όνομα του αποστολέα για να δείτε την υποκείμενη διεύθυνση ηλεκτρονικού ταχυδρομείου.
- Εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή μια τηλεφωνική κλήση είναι αμφισβητήσιμα, επικοινωνήστε απευθείας με τον αποστολέα, χρησιμοποιώντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου ή τον αριθμό τηλεφώνου που έχετε καταχωρήσει για τη συγκεκριμένη επαφή.

Πως οι κυβερνοεγκληματίες χρησιμοποιούν τα κλεμμένα δεδομένα



*Identity fraud is a serious issue. Fraudsters have stolen $112 billion in the past six years, equating to **$35,600** stolen per minute*

Source: 2016 Javelin Strategy & Research, Survey Report Results

Πως οι κυβερνοεγκληματίες χρησιμοποιούν τα κλεμμένα δεδομένα

Οι κυβερνοεγκληματίες προσπαθούν συνεχώς να κλέψουν δεδομένα και ταυτότητες:

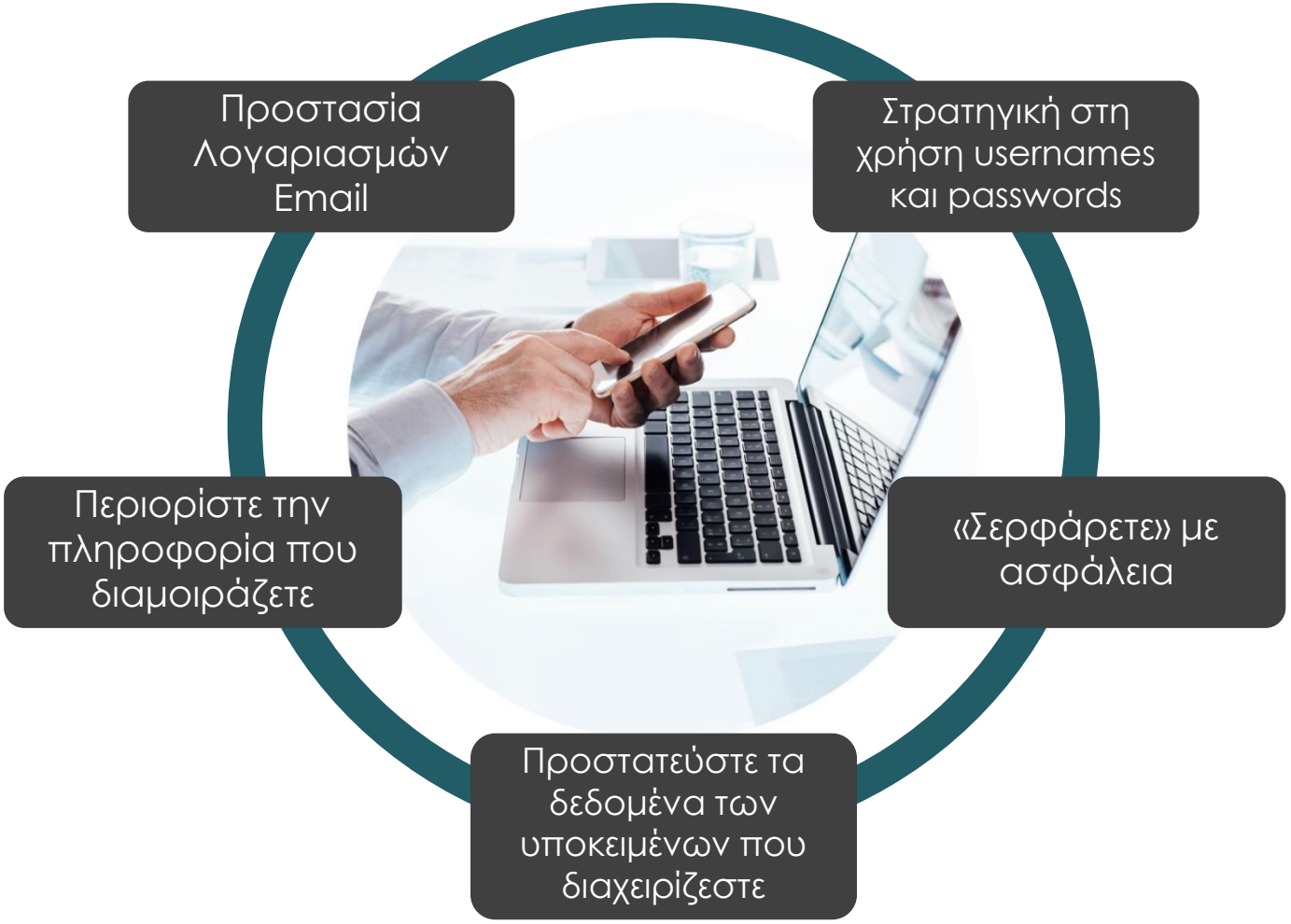
Προσωπικά Δεδομένα

- Αριθμοί Ταυτότητας
- ΑΦΜ
- Usernames
- Ημερομηνίες Γέννησης
- Κωδικοί Πρόσβασης
- Αριθμοί Πιστωτικών Καρτών
- Τραπεζικοί Λογαριασμοί
- Στοιχεία Απασχόλησης
- κ.α.

Σχετικά Κυβερνοεγκλήματα

- Δόλιες Συναλλαγές
  - αγορές
  - μεταφορές χρημάτων
- Κλοπή Ταυτότητας
  - Χρήση κλεμμένων προσωπικών δεδομένων με σκοπό την εξαπάτηση
  - Προσποίηση άλλου άτομου

Σύνοψη


Προστασία Λογαριασμών Email
Στρατηγική στη χρήση usernames και passwords
Περιορίστε την πληροφορία που διαμοιράζετε
«Σερφάρετε» με ασφάλεια
Προστατεύστε τα δεδομένα των υποκειμένων που διαχειρίζεστε

Ευχαριστώ!