Δείτε τον εαυτό σας στον κυβερνοχώρο

Έναατομικό ταξίδι στους κυβερνοκινδύνους

CYBERREADY

Ας ξεκινήσουμε →

Πριν ξεκινήσετε:

Στόχος αυτής της άσκησης είναι σας βοηθήσει να **αναγνωρίσετε** τους βασικούς κυβερνοκινδύνους, να τους **κατανοήσετε** και να τους **περιορίσετε**

#1

Χαρακτηρίστε τη **μέρα σας στη δουλειά**

#2

Ανακαλύψτε τους **κινδύνους** σας

#3

Ανακαλύψτε **πραγματικές ιστορίες**

#4

Μάθετε **τι να κάνετε**

Ας ξεκινήσουμε →

Πρώτο βήμα:

Χαρακτηρίστε τη **μέρα σας στη δουλειά**

Επόμενο →

Επιλέξτε τον χαρακτήρα με τον οποίο ταυτίζεστε:

Λαμβάνω δεκάδες **email** τη μέρα

Εργάζομαι κυρίως με **πελάτες**

Μου αρέσει να εργάζομαι σε **δημόσιους χώρους**

Διαχειρίζομαι **χρηματικές** συναλλαγές

Χαρακτηρίστε τη **μέρα σας στη δουλειά**

Ανακαλύψτε τους **κινδύνους** σας

Ανακαλύψτε **πραγματικές ιστορίες**

Μάθετε **τι να κάνετε**

Λαμβάνετε δεκάδες email τη μέρα;

Ανακαλύψτε τους **κινδύνους σας**

Επόμενο →

Οι κίνδυνοι

Η εκτεταμένη χρήση των email σας κάνει ιδιαίτερα ευάλωτους στις παρακάτω μορφές εξαπάτησης:

Ηλεκτρονικό «ψάρεμα»

Διαρροή επαγγελματικών Email (Business-Email-Compromise, BEC)

Τι σημαίνει αυτό; →

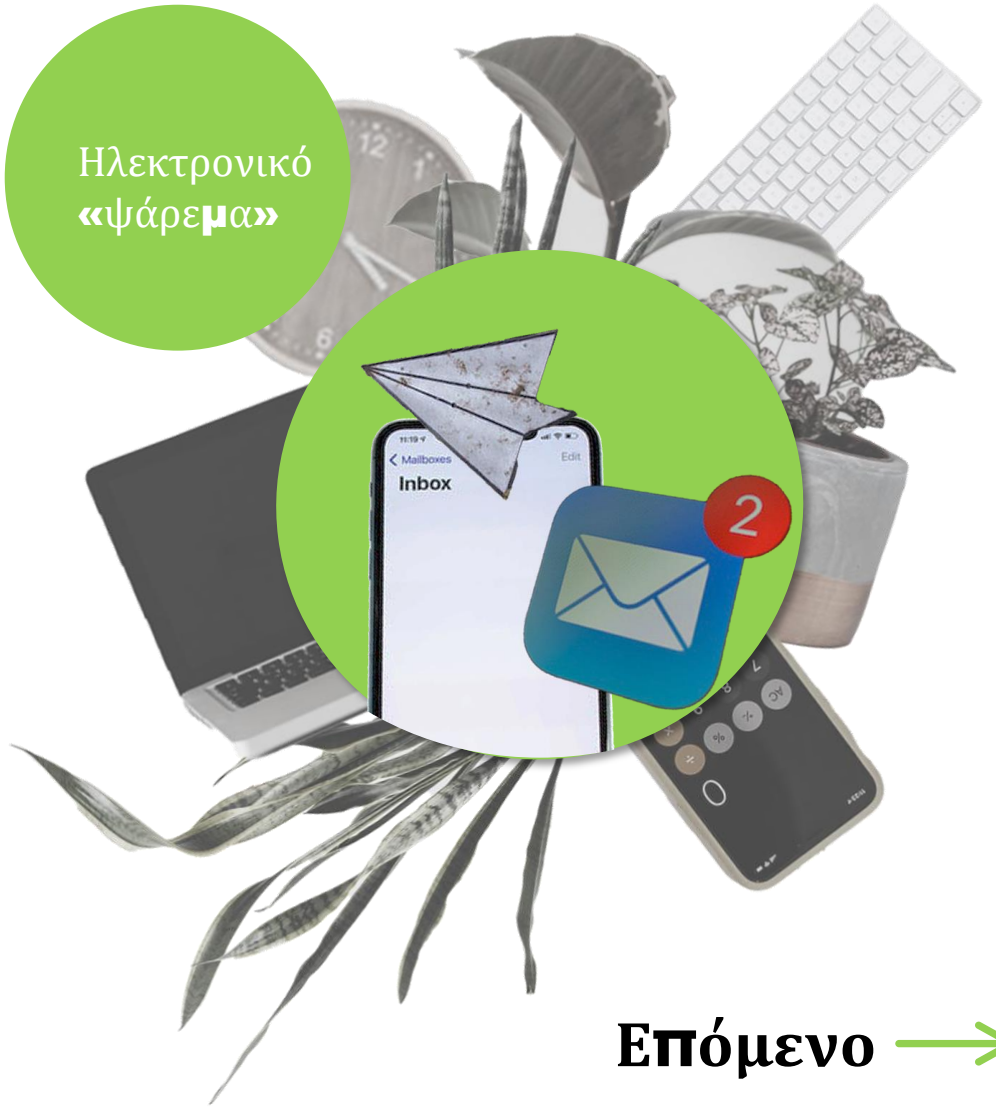
Ανακαλύψτε πραγματικές ιστορίες

Πολλοί άνθρωποι πέφτουν θύματα σε αυτές τις απάτες καθημερινά.
Ακολουθούν κάποιες από τις **ιστορίες** τους για να σας βοηθήσουν να κατανοήσετε του κινδύνους

Επόμενο →

«Ήταν μια από αυτές τις μέρες χωρίς χρόνο για καφέ. **Έλαβα ένα email** από το «Τμήμα Ανθρωπίνου Δυναμικού». Σ' αυτό περιλαμβανόταν και ένας σύνδεσμος για μία φόρμα που ζητούσε τα στοιχεία μου, συμπεριλαμβανομένου του εταιρικού μου email και του κωδικού.

Κατά το γεύμα, **ανακάλυψα πως κανείς από τους συναδέλφους μου δεν είχε λάβει αυτή τη φόρμα.** Είχα πέσει θύμα ηλεκτρονικού «ψαρέματος»;



Επόμενο →

«**Έλαβα ένα email** από έναν πελάτη που μου ζητούσε βοήθεια για να δει τα στοιχεία του. Έγραφε ότι έπρεπε να υπογράψει μια συμφωνία και χρειαζόταν γρήγορα οικονομικά στοιχεία, **γι' αυτό μοιράστηκα τις εμπιστευτικές πληροφορίες μαζί του**.

Αργότερα, όταν είδα ξανά το email, αντιλήφθηκα **ότι η διεύθυνση του email δεν ήταν σωστά γραμμένη. Ακόμα και το όνομα είχε τυπογραφικό λάθος.»**

Επόμενο →

«Έλαβα ένα **email** από τον «Ντάνι Μονέλ», το αφεντικό μου. Σ' αυτό, μου ζήτησε να **μεταφέρω χρήματα σε έναν προμηθευτή άμεσα**, καθώς είχαμε παραβιάσει το συμβόλαιο.
Αφού ολοκλήρωσα το αίτημά του άμεσα, ένιωθα ο καλύτερος υπάλληλος.

Αργότερα, όταν κοίταξα ξανά το email, αντιλήφθηκα ότι **κάτι δεν πήγαινε καθόλου καλά**.»

Επόμενο βήμα

Και τώρα, το τελευταίο βήμα:

Μάθετε τι να κάνετε 

4 συμβουλές για το πώς να μειώσετε τους κινδύνους σας

#1 **Ελέγξτε** τη διεύθυνση email του αποστολέα και επαληθεύστε ότι είναι αυτή που περιμένετε

#2 **Επικοινωνήστε με το άτομο που έστειλε το αίτημα** σε ξεχωριστό μήνυμα ή κανάλι (όταν έχετε υποψίες)

#3 Κάντε κατάδειξη με το ποντίκι πάνω από τους συνδέσμους για να επιβεβαιώσετε ότι τα URL οδηγούν σε γνωστή σελίδα (στα κινητά, πατώντας παρατεταμένα στον σύνδεσμο θα εμφανιστεί η διεύθυνση του ιστοτόπου)

#4 **Να είστε προσεκτικοί με email που σας ζητούν να δράσετε γρήγορα.** Αυτά θα πρέπει να αποτελούν προειδοποιητικό σημάδι.

Ολοκλήρωση →

Εργάζεστε με πελάτες;

Ανακαλύψτε τους **κινδύνους σας**

Επόμενο →

Οι κίνδυνοι

Η συναναστροφή με πολλούς ανθρώπους (π.χ. σε ρόλους εξυπηρέτησης πελατών) σας κάνει ιδιαίτερα ευάλωτους σε τέτοιους κινδύνους:

Απάτη πλαστοπροσωπίας

Κοινοποίηση εμπιστευτικών πληροφοριών

Τι σημαίνει αυτό; →

Ανακαλύψτε πραγματικές ιστορίες

Πολλοί άνθρωποι πέφτουν θύματα σε αυτές τις απάτες καθημερινά.
Ακολουθούν κάποιες από τις **ιστορίες** τους για να σας βοηθήσουν να κατανοήσετε του κινδύνους

Επόμενο →

«**Έλαβα ένα email** από τον «Μπεν» από το λογιστήριο του πελάτη, στο οποίο ζητούσε κάποια αρχεία για ένα έργο πάνω στο οποίο δούλευα. **Οπότε τα έστειλα**.

Μόνο όταν έγινε μήνυση στην εταιρία μου **ανακάλυψα πως δεν υπήρχε κανένας Μπεν στη λίστα προσωπικού του πελάτη**.»

Επόμενο →

«**Το αφεντικό μου μού ζήτησε να στείλω το λογιστικό φύλλο με τα ετήσια έσοδα** στον Μάικλ από το Οικονομικό Τμήμα και **το έκανα**. Μία εβδομάδα αργότερα, ήταν στις ειδήσεις.

Φαίνεται πως κατά λάθος το έστειλα σε κάποιον Μάικλ σε κάποια άλλη εταιρία.»

Επόμενο →

«**Μια γυναίκα με πήρε τηλέφωνο** κλαίγοντας, ζητώντας το ιστορικό των κλήσεων του δεκατριάχρονου γιου της που αγνοούνταν. **Ένιωσα άμεση ανάγκη να την βοηθήσω** χωρίς να την επιβαρύνω με πολλές ερωτήσεις.

Αφού έγινε μήνυση στην εταιρία, ανακάλυψα ότι **έστειλα τις πληροφορίες σε έναν πράκτορα ιδιωτικών ερευνών** που ερευνούσε την απιστία του συζύγου της.

Επόμενο βήμα

Και τώρα, το τελευταίο βήμα:

Μάθετε τι να κάνετε 

4 συμβουλές για το πώς να μειώσετε τους κινδύνους σας

#1 **Επαληθεύετε πάντοτε** την ταυτότητα του ατόμου με το οποίο συνομιλείτε

#2 Προτού κοινοποιήσετε πληροφορίες ενός πελάτη, **βεβαιωθείτε** ότι οι πληροφορίες αυτές μπορούν να κοινοποιηθούν

#3 Κοινοποιείτε ευαίσθητες πληροφορίες **μόνο μέσω ορισμένων καναλιών**

#4 Προσέχετε τον **τόνο φωνής του αιτούντος**. Αν κάποιος προσπαθεί να σας πιέσει, αυτό είναι συνήθως σημάδι απάτης

Ολοκλήρωση →

Εργάζεστε σε δημόσιους χώρους;

Ανακαλύψτε τους **κινδύνους σας**

Επόμενο →

Οι κίνδυνοι

Η εργασία σε δημόσιους χώρους σας κάνει ιδιαίτερα ευάλωτους σε τέτοιους κινδύνους:

Κλοπή φορητού υπολογιστή

Κρυφάκουσμα

Επιθέσεις μέσω Wi-Fi

Τι σημαίνει αυτό; →

Ανακαλύψτε πραγματικές ιστορίες

Πολλοί άνθρωποι πέφτουν θύματα σε αυτές τις απάτες καθημερινά.
Ακολουθούν κάποιες από τις **ιστορίες** τους για να σας βοηθήσουν να κατανοήσετε του κινδύνους

Επόμενο →

«Εκείνη τη μέρα στο **τρένο** είχε πολύ κόσμο. Εφόσον είχα να ολοκληρώσω μια σημαντική αναφορά, **εργάστηκα στον φορητό υπολογιστή μου**. Την επόμενη μέρα, βρήκα μια ανάρτηση στο Reddit, η οποία περιείχε **εσωτερικές πληροφορίες για την εταιρία μας, οι οποίες αναφερόταν στο έγγραφό μου**.

Είναι δυνατόν να ήμουν εγώ υπεύθυνη για τη **διαρροή**;

Επόμενο →

«Μια μέρα, ενώ εργαζόμουν σε μια καφετέρια που πηγαίνω συχνά, **σηκώθηκα** για να πάρω κάτι να φάω και **άφησα τον υπολογιστή μου ανεπιτήρητο για μια στιγμή**.

Όταν επέστρεψα, **δεν ήταν εκεί**.»

Επόμενο →

«Στο δρόμο μου για τον πελάτη, έπρεπε να ελέγξω κάποιες λεπτομέρειες. **Γι' αυτό συνδέθηκα στο ελεύθερο Wi-Fi της διπλανής καφετέριας**, έλεγξα και το έκλεισα.

Τον επόμενο μήνα, **έγινε μια εισβολή στο σύστημά μας** μέσω του χρήστη μου. Δεν μπορώ να βγάλω από το μυαλό μου το ενδεχόμενο να προκλήθηκε από τη χρήση αμφίβολου Wi-Fi.»

Επόμενο βήμα

Και τώρα, το τελευταίο βήμα:

Μάθετε τι να κάνετε 

3 συμβουλές για το πώς να μειώσετε τους κινδύνους σας

#1 **Κρατάτε τον φορητό υπολογιστή δίπλα σας** κάθε στιγμή. Θα εκπλαγείτε από τον αριθμό των υπολογιστών που κλέβονται κάθε χρόνο.

#2 **Χρησιμοποιείτε μόνο ιδιωτικές συνδέσεις δικτύου**, ποτέ δημόσιες.

#3 Βεβαιωθείτε ότι **μόνο εσείς μπορείτε να δείτε την οθόνη** του φορητού υπολογιστή και τις σημειώσεις σας

Ολοκλήρωση →

Διαχειρίζεστε χρηματικές συναλλαγές;

Ανακαλύψτε τους **κινδύνους σας**

Επόμενο →

Οι κίνδυνοι

Η κατοχή δικαιωμάτων διεκπεραίωσης τραπεζικών συναλλαγών σας κάνει ιδιαίτερα ευάλωτους στις παρακάτω μορφές εξαπάτησης:

Διαρροή επαγγελματικών Email (Business-Email-Compromise, BEC)

Απάτη πλαστοπροσωπίας προμηθευτή

Τι σημαίνει αυτό; →

Ανακαλύψτε πραγματικές ιστορίες

Πολλοί άνθρωποι πέφτουν θύματα σε αυτές τις απάτες καθημερινά.
Ακολουθούν κάποιες από τις **ιστορίες** τους για να σας βοηθήσουν να κατανοήσετε του κινδύνους

Επόμενο →

«**Έλαβα ένα email** από το αφεντικό μου στο οποίο μου ζητούσε να **μεταφέρων 17.000 δολάρια σε έναν νέο προμηθευτή**. Έγραφε, «Είμαι σε διάσκεψη. δεν μπορώ να μιλήσω. **Παρακαλώ να κάνεις τη μεταφορά ΑΜΕΣΑ**», έτσι κι έκανα.

Μια μέρα αργότερα, στο γραφείο, συνειδητοποίησα ότι **δεν είχε ιδέα σε τι αναφερόμουν**.»

Επόμενο →

«**Έλαβα ένα email** από τον **νέο διαχειριστή οικονομικών** ενός προμηθευτή μας που μου ζητούσε οι **μελλοντικές πληρωμές** να γίνονται σε διαφορετικό τραπεζικό λογαριασμό. **Έτσι κι έκανα**.

Ήταν **απάτη**, αλλά πώς να το ξέρω;»

Επόμενο →

«**Έλαβα ένα email** από το Τμήμα Ανθρώπινου Δυναμικού που περιείχε μία μακριά συνομιλία. Ζητούσαν να **αγοράσω δωροκάρτες** για την πρωτοχρονιάτικη γιορτή. Το μόνο που χρειαζόταν ήταν οι αριθμοί τους. Επομένως, **αγόρασα τις κάρτες και έστειλα τους αριθμούς**.

Όπως προέκυψε, ήταν απάτη και **τα λεφτά είχαν κάνει φτερά**.»

Επόμενο βήμα

Και τώρα, το τελευταίο βήμα:

Μάθετε τι να κάνετε 

3 συμβουλές για το πώς να μειώσετε τους κινδύνους σας

#1 **Ελέγξτε** τη διεύθυνση email του αποστολέα. Αν είναι διαφορετική απ' ότι συνήθως, κλείστε το email και επικοινωνήστε με τον εικαζόμενο αποστολέα με άλλον τρόπο

#2 **Επιβεβαιώστε οποιαδήποτε αλλαγή** στον τρόπο πληρωμής με το σύνηθες άτομο επικοινωνίας, πρόσωπο με πρόσωπο ή μέσω τηλεφώνου

#3 **Ελαττώστε ταχύτητα.** Οι εισβολείς προσπαθούν να κάνουν τους ανθρώπους να δρουν γρήγορα ώστε να μην αντιληφθούν τα ανησυχητικά σημάδια ή να συμβουλευτούν άλλους.

Ολοκλήρωση →

Τέλεια! Ολοκληρώσατε το ταξίδι

Τι θα θέλατε να κάνετε τώρα;

Εξερευνήστε άλλο ταξίδι

Τέλος

Ευχαριστούμε για τη συμμετοχή σας

Ελπίζουμε να διασκεδάσατε και να λάβατε χρήσιμες πληροφορίες
από την εμπειρία που χτίσαμε