

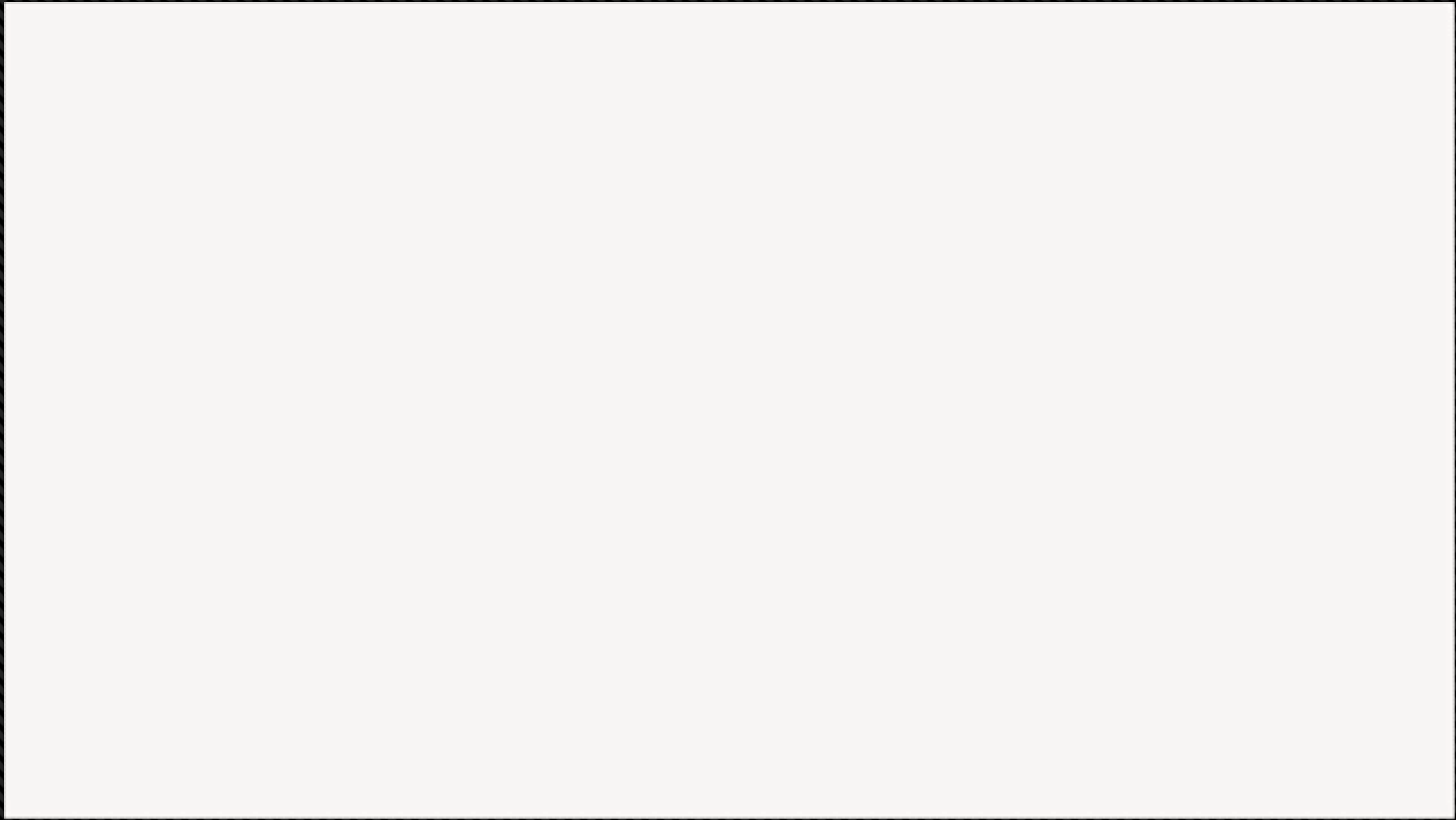
# Διδακτική παρέμβαση

- Τίτλος: Phishing & Pharming
- Τάξη: Α' Γυμνασίου
- Μάθημα: Πληροφορική
- Ενότητα: Διαδίκτυο
- Χρονική διάρκεια: 2 διδακτικές ώρες
- Στόχοι:
  - Οι μαθητές να γνωρίσουν τις έννοιες Phishing & Pharming και την επικινδυνότητα της κάθε έννοιας
  - Οι μαθητές να είναι σε θέση να εντοπίσουν μία απάτη Phishing

# Phishing & Pharming

Καρακίε Βασιλική





# Phishing: Τι είναι;

Με τον όρο ηλεκτρονικό ψάρεμα (phishing) περιγράφεται η προσπάθεια που καταβάλλει κάποιος όταν με διάφορους τρόπους προσπαθεί να αποσπάσει από εσένα προσωπικά σου στοιχεία στο διαδίκτυο. Συνήθως γίνεται μέσω ηλεκτρονικού ταχυδρομείου (email) και ο πραγματικός αποστολέας δεν είναι αυτός που φαίνεται.

Οι πληροφορίες που έχουν κλαπεί από τα θύματα, συνήθως χρησιμοποιούνται για το άδειασμα των τραπεζικών λογαριασμών τους ή πωλούνται στη μαύρη αγορά του internet.

# Phishing: Παραδείγματα 1/2

- Μπορεί να λάβεις ένα μήνυμα ηλεκτρονικού ταχυδρομείου από μια ιστοσελίδα που χρησιμοποιείς και μέσω του οποίου να σου ζητάνε να δώσεις κάποια προσωπικά σου στοιχεία για λόγους ασφαλείας
- Μπορεί να λάβεις ένα μήνυμα που να υποστηρίζει ότι κέρδισες ένα σημαντικό ποσό και να σε προτρέπει να δώσεις τα προσωπικά σου στοιχεία για να λάβεις τα χρήματα.
- Μπορεί να σου ζητήσουν να πατήσεις σε κάποιο σύνδεσμο ο οποίος όμως στην πραγματικότητα δεν είναι αθώος και με αυτό τον τρόπο γίνεται εγκατάσταση κακόβουλου ή κατασκοπευτικού λογισμικού στον υπολογιστή σου.
- Μπορεί να λάβεις ένα μήνυμα που υποτίθεται είναι από κάποια γνωστή τράπεζα, οργανισμό, τηλεπικοινωνιακό πάροχο ή άλλη νόμιμη εταιρεία που ενημερώνει τους παραλήπτες του για την ύπαρξη κενών ασφαλείας σε κάποιο λογαριασμό ή συνδρομή και ζητάει τα στοιχεία σου.

# Phishing: Παραδείγματα 2/2

έχετε νέα επιστροφή φόρου

**ΠΑΡΑΠΛΑΗΤΙΚΟ  
EMAIL  
PHISHING**

Gov.gr Wallet

Σας γράφω για να σας ενημερώσω ότι η Ελληνική Φορολογική Υπηρεσία υπολόγισε τη φορολογική σας δήλωση και αποφάσισε ότι δικαιούστε επιστροφή φόρου ύψους 634,13 ευρώ.

Παρακαλούμε κάντε κλικ στον παρακάτω σύνδεσμο για να επαληθεύσετε τα στοιχεία σας, ώστε να ξεκινήσουμε την επεξεργασία της επιστροφής σας. Αυτό θα εγγυηθεί ότι ο σωστός λογαριασμός θα λάβει την επιστροφή

**Επιβεβαιώστε τα στοιχεία σας.**

Θα ξεκινήσουμε την επεξεργασία της επιστροφής σας μόλις έχουμε όλες τις πληροφορίες που θέλουμε από εσάς. Τα χρήματα ενδέχεται να μην εμφανιστούν στο λογαριασμό σας για έως και 2 ημέρες, οπότε παρακαλούμε να το γνωρίζετε αυτό.

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ  
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΟΙΚΟΝΟΜΙΚΗΣ

Μετά από τον τελευταίο ετήσιο υπολογισμό της φορολογικής δραστηριότητάς σας έχουμε καθορίσει ότι είστε επιλέξιμοι για να λάβετε μια επιστροφή φόρου 568.24 ευρώ. Παρακαλώ συμπληρώστε το έντυπο.

Ο τραπεζικός χρήστης Διαδικτύου σας - ταυτότητα:  Ο αριθμός τραπεζικού λογαριασμού σας:

Ο τραπεζικός κωδικός πρόσβασης Διαδικτύου σας:  Ο αριθμός δρομολόγησης τράπεζάς σας:

Το όνομά σας:  - (Τυπώστε το πλήρες όνομα σας) Ο εύρων αριθμός ταυτότητάς σας:

Η διεύθυνση κατοικίας σας  Κράτος:  Ο αριθμός Α.Φ.Μ. σας:

Τεχνολογικός κωδικός:  Πάλη:

Το ποσό 568.24 ευρώ θα είναι επένει στην κάρτα μου.

Επιλέξτε το οικονομικό όργανο σας:  ή γράψτε το οικονομικό όργανο σας

Αριθμός καρτών:  Ο απολογισμός όπου θέλετε να λάβετε την επιστροφή φόρου 568.24

Ημερομηνία λήξης:  -3 μήνες στο πίσω μέρος της κάρτας σας

Καρπίτσα:  - Εκτύπωση τον ψηφιακό αριθμό αναγνώρισης του ATM προσωπικό για την επεξεργασία και την απολήτευση τραπεζιών

Σημαντικός: Ο φορολογικός νόμος επιβάλλει τις βαριές ποινικές ρητρες για το δόσιμο των ψεύτικων ή παραπλανητικών πληροφοριών

Δηλώνω ότι: όλες οι πληροφορίες που έχω δώσει σε αυτήν την φορολογική επιστροφή, συμπεριλαμβανομένων οποιωνδήποτε ει συνδέσας, είναι αληθινές και σωστές

# Phishing: Διαφορετικά είδη

## ○ **Απάτες μέσω email**

- Σε εξαπατούν για να μοιραστείς προσωπικές πληροφορίες
- Σε οδηγούν να κατεβάσεις επικίνδυνο κακόβουλο λογισμικό

## ○ **SMiShing**

Το SMiShing είναι παρόμοιο με την απάτη μέσω ηλεκτρονικού ταχυδρομείου, αλλά ξεγελά τους χρήστες μέσω μηνυμάτων κειμένου

## ○ **Spear Phishing**

Το spear phishing στοχεύει σε ένα συγκεκριμένο άτομο. Ενδέχεται να δεις μια σειρά μηνυμάτων ηλεκτρονικού ταχυδρομείου που θα σε παρασύρουν να αναλάβεις δράση.

## ○ **Whaling**

Το whaling απευθύνεται επίσης σε ένα άτομο ή έναν οργανισμό. Ωστόσο, είναι συνήθως κάποιος που έχει πολλά να χάσει, όπως διευθυντές, προσωπικότητες, πολιτικά πρόσωπα ή πλούσιες οικογένειες.



# Phishing: Πώς να εντοπίσεις μια απάτη

- Μιμείται έμπιστες μάρκες
- Έχουν συντακτικά και ορθογραφικά λάθη
- Χρησιμοποιούν τακτικές εκφοβισμού
- Είναι απεσταλμένο από ανεπίσημη διεύθυνση email
- Είναι “Πολύ καλό για να είναι αληθινό”



# Phishing: Συμβουλές για να προστατευτώ

- Να είστε καχύποπτοι όταν σας ζητούν μέσω μεμονωμένων e-mail προσωπικές πληροφορίες
- Μη συμπληρώνετε φόρμες με τα προσωπικά σας στοιχεία όταν σας αποστέλλονται από άγνωστες διευθύνσεις ηλεκτρονικών ταχυδρομείων
- Πληκτρολογήστε στον browser τη διεύθυνση της ιστοσελίδας και μη μπαίνεται σε αυτή μέσω υπερσυνδέσμων
- Προστάτευσε τον υπολογιστή σου από κακόβουλο λογισμικό (antivirus, antispram, antispyware).
- Εμπιστέψου το ένστικτό σου. Αν έχεις αμφιβολία για κάποια ιστοσελίδα ή σύνδεσμο απλά μην το ακολουθήσεις!

# Pharming: Τι είναι;

- Το Pharming είναι μια μορφή απάτης της ηλεκτρονικής διεύθυνσης (domain name) που έχει ως αποτέλεσμα να πιστεύουν οι χρήστες ότι βρίσκονται σε μια γνήσια ιστοσελίδα με το σωστό URL. Ωστόσο, στην πραγματικότητα έχουν παραπεμφθεί σε μια ψεύτικη, η οποία όμως μοιάζει πανομοιότυπη με τη γνήσια.
- Εκμεταλλεζόμενοι κάποια κενά στην ασφάλεια μιας ιστοσελίδας στην οποία οι χρήστες μπαίνουν για να πραγματοποιήσουν διάφορες συναλλαγές, οι απατεώνες καταφέρνουν να εκτρέψουν την ροή των επισκεπτών σε άλλο ιστοχώρο, όπου τα στοιχεία των συναλλαγών που καταχωρούνται χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών.
- Τέτοιου είδους εκτροπή δεν μπορεί να γίνει σε ιστοσελίδες που χρησιμοποιούν το πρωτόκολλο SSL. Για να διαπιστώσετε αν οι συναλλαγές που κάνετε είναι ασφαλείς, δείτε στο πεδίο της διεύθυνσης αν υπάρχει η ένδειξη `https://` αντί για το συμβατικό `http://`.

# Pharming Vs Phishing

- Το Pharming εστιάζει περισσότερο στην επίθεση στο σύστημα *DNS*.
- Το Phishing εστιάζει περισσότερο στη χειραγώγηση των χρηστών.

# Pharming: Πώς ξέρετε αν είστε θύμα

- Οι κωδικοί πρόσβασης στον τραπεζικό σας λογαριασμό στο διαδίκτυο άλλαξαν χωρίς να ξεκινήσετε τη δράση.
- Υπάρχουν μηνύματα ή αναρτήσεις στον λογαριασμό σας στο Facebook που δεν δημιουργήσατε.
- Έγιναν ανεξήγητες χρεώσεις στην πιστωτική σας κάρτα.
- Έχουν εγκατασταθεί περίεργες εφαρμογές στον υπολογιστή σας τις οποίες ούτε κατεβάσατε ούτε εγκαταστήσατε.
- Οι λογαριασμοί σας στα μέσα κοινωνικής δικτύωσης έχουν στείλει αιτήματα φιλίας που δεν υποβάλατε.

# Πηγές

- <https://www.eset.com/gr/phishing/>
- <https://saferinternet4kids.gr/hot-topics-ef/phishing-ef/>
- <https://cyberalert.gr/phising/>
- <https://www.saferinternet.gr/index.php?objId=Category116&parentobjId=Page2>
- <https://www.microsoft.com/el-gr/security/business/security-101/what-is-phishing>
- <https://www.aade.gr/asfaleia-psifiakon-ypiresion-imerominia-enimerosis-04072023>
- <https://www.ssl.com/el/%CE%B9%CF%83%CF%84%CE%BF%CE%BB%CF%8C%CE%B3%CE%B9%CE%B1/%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%86%CE%B1%CF%81%CE%BC%CE%B1%CE%BA%CE%B5%CF%85%CF%84%CE%B9%CE%BA%CE%AE/>
- <https://el.safetydetectives.com/blog/%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-phishing-%CE%B1%CF%80%CE%BB%CF%8C%CF%82-%CE%BF%CE%B4%CE%B7%CE%B3%CF%8C%CF%82-%CE%BC%CE%B5-%CF%80%CE%B1%CF%81%CE%B1%CE%B4%CE%B5%CE%AF%CE%B3/#spotting>

# Δραστηριότητες για την επόμενη διδακτική ώρα

1. Αφού παρακολουθήσετε το βίντεο της διαφάνειας 2 να συζητήσετε όλοι μαζί μέσα την τάξη αν γνωρίζετε περιστατικά υποψήφιων θυμάτων phishing και πως αντέδρασαν αυτοί; Κατάλαβαν την απόπειρα phishing; Αν ναι, τι ήταν αυτό που πρόδωσε τους phishers στην κάθε περίπτωση;
2. Θα χωριστείτε σε ομάδες των δύο ατόμων. Αφού συζητήσετε μεταξύ σας θα γράψετε μία παράγραφο η κάθε ομάδα που θα απαντάτε στην ερώτηση «ποιο θεωρείτε ποιο επικύνδυνο για εσάς; Το phishing ή το pharming και γιατί;»