Co-funded by the Erasmus+ Programme of the European Union

Phishing and how to avoid it
(ηλεκτρονικό) Ψάρεμα και πώς να το αποφύγετε

English	Greek
What is phishing?	**Τι είναι το (ηλεκτρονικό) ψάρεμα;**
Phishing is a fraudulent attempt to obtain any type of sensitive information or data that can be used to attack unsuspecting users. The offender tries to disguise their self as a trust worthy entity usually via an email, or an SMS, or instant messaging and somehow extract personal information from the victims by asking them to complete a form or visit a (malicious) website.	Το ηλεκτρονικό ψάρεμα (phishing) είναι μια δόλια προσπάθεια απόκτησης κάθε είδους ευαίσθητων πληροφοριών ή δεδομένων που μπορούν να χρησιμοποιηθούν για την επίθεση ανυποψίαστων χρηστών. Ο δράστης προσπαθεί να μεταμφιεστεί σε αξιόπιστη οντότητα συνήθως μέσω email, SMS ή άμεσων μηνυμάτων και με κάποιο τρόπο να εκμαιεύσει προσωπικές πληροφορίες από τα θύματα ζητώντας τους να συμπληρώσουν μια φόρμα ή να επισκεφθούν έναν (κακόβουλο) ιστότοπο.
Types of phishing (according to (Wikipedia, 2020)**)**	**Τύποι**
- Spear phishing: directed at specific individuals or companies (employees and executives) - Whaling: specifically spear phishing executives of companies - Catphishing: online deception involving getting to know the 'victim' personally - Clone phishing: creating a fraudulent communication based on an intercepted original and replacing legitimate links or files with malicious ones - Voice phishing: tricking users to call a 'bank' service in order to perform some task or update some information - SMS phishing (or smishing): target receives an SMS with a link or being asked to call a phone number, or send an email or an SMS.	- Spear phishing: απευθύνεται σε συγκεκριμένα άτομα ή εταιρείες (υπαλλήλους και στελέχη) - Φαλαινοθηρία: ειδικά sprear phishing στελεχών μιας εταιρίας - Catphishing: διαδικτυακή εξαπάτηση που περιλαμβάνει την προσωπική γνωριμία με το «θύμα» - Κλωνοποίηση ηλεκτρονικού ψαρέματος: δημιουργία ψευδούς επικοινωνίας που βασίζεται σε πρωτότυπο με αντικατάσταση νόμιμων συνδέσμων ή αρχείων με κακόβουλους - Φωνητικό ηλεκτρονικό ψάρεμα (phishing): εξαπατώντας τους χρήστες να καλέσουν μια υπηρεσία «τράπεζας» προκειμένου να εκτελέσουν κάποια εργασία ή να ενημερώσουν κάποιες πληροφορίες - SMS ηλεκτρονικού ψαρέματος (ή smishing): ο "στόχος" (υποψήφιο θύμα) λαμβάνει ένα SMS με έναν σύνδεσμο ή του ζητείται να καλέσει έναν αριθμό τηλεφώνου ή να στείλει ένα email ή ένα SMS.
Techniques used	**Τεχνικές που χρησιμοποιούνται**
- Link manipulation: making a link go somewhere or do something that can compromise or extract sensitive information - Filter evasion: manipulating e-mail contents so as to avoid filters placed on e-mail servers - Website forgery: using web programming techniques to trick users into thinking they are visiting a legitimate site when in fact they are not.	- Χειρισμός συνδέσμου: κάνοντας έναν σύνδεσμο να πάει κάπου ή να κάνει κάτι που μπορεί να θέσει σε κίνδυνο ή να εξαγάγει ευαίσθητες πληροφορίες - Διαφυγή φίλτρου: χειρισμός περιεχομένου e-mail ώστε να αποφεύγονται τα φίλτρα που τοποθετούνται σε διακομιστές e-mail - Πλαστογραφία ιστοτόπου: χρήση τεχνικών προγραμματισμού ιστού για να εξαπατήσει τους χρήστες να πιστεύουν ότι επισκέπτονται έναν

- Covert redirect: attackers manipulate links to appear legitimate but they direct to malicious sites. - Social engineering: users are encouraged to click on links or open attachments	νόμιμο ιστότοπο, ενώ στην πραγματικότητα δεν είναι. - Κρυφή ανακατεύθυνση: οι εισβολείς χειρίζονται συνδέσμους για να φαίνονται νόμιμοι, αλλά μεταφέρουν τον χρήστη σε κακόβουλους ιστότοπους. - Social engineering οι χρήστες ενθαρρύνονται να κάνουν κλικ σε συνδέσμους ή να ανοίξουν συνημμένα
How to avoid phishing	**Πως να αποφύγετε το (ηλεκτρονικό) ψάρεμα**

- On a big scale
  o Big mail service providers include anti-spam and anti-phishing filters to stop messages before they even reach the servers
  o System administrators can equip the mail server with anti-phishing filters
  o There are quite a few websites that report the details of phishing attempts. One example is: FraudWatch International
  o Larger companies tend to train employees to recognize popular phishing attempts
 	
- On a user level:
- **ALWAYS PAY ATTENTION**
  o Never open emails from people you do not know
  o If you do open the email **read it carefully** and pay attention to details like, legitimacy of the sender address, proper use of the English language, existence of vague (rather than specific) information.
  o Never click on attachments from emails that you were not expecting. If the original sender appears to be legitimate, contact them directly and ask them if they sent you anything
  o Never click on email links included in emails that you were not expecting. If an email appears legitimate and is asking you to verify your details, don't click the link. Go the company's website and try and find a page or notification about that verification process
  o Never call a number just because an email or SMS or instant message says so. Contact the main switchboard of the company and ask to be connected to whoever 'allegedly' sent you the communication
  o Any communication claiming that you have won some competition or you are the lucky draw winner can surely be considered a phishing attempt.
  o Any communication informing you of a suspension of service and an urgency to update your details in order to protect your
	- Σε μεγάλη κλίμακα
	  o Οι μεγάλοι πάροχοι υπηρεσιών αλληλογραφίας περιλαμβάνουν φίλτρα anti-spam και anti-phishing για να σταματήσουν τα μηνύματα πριν φτάσουν ακόμη και στους διακομιστές
	  o Οι διαχειριστές συστήματος μπορούν να εξοπλίσουν τον διακομιστή αλληλογραφίας με φίλτρα anti-phishing
	  o Υπάρχουν αρκετοί ιστότοποι που αναφέρουν τις λεπτομέρειες των προσπαθειών ηλεκτρονικού ψαρέματος. Ένα παράδειγμα είναι: FraudWatch International
	  o Οι μεγαλύτερες εταιρείες τείνουν να εκπαιδεύουν τους υπαλλήλους να αναγνωρίζουν δημοφιλείς απόπειρες ηλεκτρονικού ψαρέματος
	
	- Σε επίπεδο χρήστη:
	- **ΠΆΝΤΑ ΝΑ ΕΊΣΤΕ ΠΡΟΣΕΚΤΙΚΟΙ**
	  o Μην ανοίγετε ποτέ μηνύματα ηλεκτρονικού ταχυδρομείου από άτομα που δεν γνωρίζετε
	  o Εάν ανοίξετε το email, διαβάστε το προσεκτικά και δώστε προσοχή σε λεπτομέρειες όπως, νομιμότητα της διεύθυνσης αποστολέα, σωστή χρήση της γλώσσας, ύπαρξη ασαφών (και όχι συγκεκριμένων) πληροφοριών.
	  o Ποτέ μην κάνετε κλικ σε συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου που δεν περιμένατε. Εάν ο αρχικός αποστολέας φαίνεται να είναι νόμιμος, επικοινωνήστε απευθείας μαζί του και ρωτήστε εάν σας έστειλε κάτι
	  o Μην κάνετε ποτέ κλικ σε συνδέσμους email που περιλαμβάνονται σε email που δεν περιμένατε. Εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου φαίνεται νόμιμο και σας ζητά να επαληθεύσετε τα στοιχεία σας, μην κάνετε κλικ στον σύνδεσμο. Μεταβείτε στον ιστότοπο της εταιρείας και δοκιμάστε να βρείτε μια σελίδα ή ειδοποίηση σχετικά με αυτήν τη διαδικασία επαλήθευσης

details can surely be considered a phishing attempt.	○ Ποτέ μην καλείτε έναν αριθμό μόνο και μόνο επειδή το λέει ένα email ή ένα SMS ή ένα άμεσο μήνυμα. Επικοινωνήστε με τον τηλεφωνικό κέντρο της εταιρείας και ζητήστε να συνδεθείτε με όποιον σας φέρεται να σας έστειλε την επικοινωνία ○ Κάθε επικοινωνία που ισχυρίζεται ότι έχετε κερδίσει κάποιο διαγωνισμό ή ότι είστε ο τυχερός νικητής κλήρωσης μπορεί σίγουρα να θεωρηθεί απόπειρα ηλεκτρονικού ψαρέματος. ○ Οποιαδήποτε επικοινωνία που σας ενημερώνει για αναστολή υπηρεσίας και σας ζητά να ενημερώσετε επειγόντως τα στοιχεία σας προκειμένου να προστατεύσετε τα στοιχεία σας μπορεί σίγουρα να θεωρηθεί απόπειρα ηλεκτρονικού ψαρέματος.
Videos (on YouTube) for identifying phishing:	**Βίντεο (στο YouTube) για τον προσδιορισμό του ηλεκτρονικού ψαρέματος:**
- Google's: Stay Safe from Phishing and Scams - Atomic Shrimp: How to recognize a phishing scan message	- Google's: Stay Safe from Phishing and Scams - Atomic Shrimp: How to recognize a phishing scan message