CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

Πρακτική μη τυπικής εκπαίδευσης:

Ηλεκτρονικό «ψάρεμα» (Phishing)

Α2 ΕΡΓΑΛΕΙΟΘΗΚΗ CYBER

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

#9	**Κάτι μοιάζει να είναι περίεργο**
Απειλή	Ηλεκτρονικό «ψάρεμα» (Phishing)
	Οι επιθέσεις ηλεκτρονικού «ψαρέματος» συχνά περιλαμβάνουν δόλια μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα ή ιστότοπους που συχνά υποδύονται νόμιμους οργανισμούς, όπως τράπεζες, πλατφόρμες κοινωνικής δικτύωσης ή κυβερνητικές υπηρεσίες κ.ά. Αυτές οι παραπλανητικές επικοινωνίες συνήθως προτρέπουν τους παραλήπτες να αποκαλύψουν εμπιστευτικές πληροφορίες, όπως διαπιστευτήρια σύνδεσης ή αριθμούς οικονομικών λογαριασμών, με ψευδείς προφάσεις. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν αυτές τις κλεμμένες πληροφορίες για να διαπράξουν κλοπή ταυτότητας, οικονομική απάτη ή άλλες κακόβουλες δραστηριότητες, θέτοντας σημαντικούς κινδύνους για την ιδιωτική ζωή των ατόμων (Κλοπή ταυτότητας και απάτη), τα οικονομικά και την ασφάλεια στο διαδίκτυο.
Τυπολογία	Ασκήσεις προσομοίωσης
Διάρκεια	2x40 λεπτά
Παρακολούθηση	Δια ζώσης – σε τάξη
Σκοπός	Αυτό το μάθημα μοιράζεται τον τρόπο με τον οποίο οι επιτήδειοι μπορούν να προσπαθήσουν να αποκτήσουν προσωπικές πληροφορίες μέσω του phishing. Πολλές φορές, η ηλεκτρονική επικοινωνία, όπως τα μηνύματα ηλεκτρονικού ταχυδρομείου και τα γραπτά μηνύματα, μπορεί να φαίνεται ότι προέρχεται από μια αξιόπιστη πηγή, αλλά στην πραγματικότητα είναι απατηλή.
Μαθησιακά αποτελέσματα	Αφού συμμετάσχουν σε αυτό το μάθημα, οι εκπαιδευόμενοι θα είναι σε θέση να: - Να αναγνωρίζουν τα χαρακτηριστικά της αξιόπιστης ηλεκτρονικής επικοινωνίας - Να εξηγούν τη σημασία της γνώσης του τρόπου αποφυγής των προσπαθειών ηλεκτρονικού «ψαρέματος» (phishing) - Να διακρίνουν μεταξύ νόμιμων και δόλιων μηνυμάτων και προσπαθειών ηλεκτρονικού «ψαρέματος» (phishing)
Προφίλ εκπαιδευόμενου	13-17 χρόνια
Αρ. Συμμετεχόντων	Ιδανικά μέχρι 20 συμμετέχοντες ή μαθητές το πολύ μιας τάξης.
Εργαλεία	• Εκτυπωμένα παραδείγματα ηλεκτρονικού «ψαρέματος» (δείτε στο παράρτημα, ή μπορείτε να εκτυπώσετε τα επόμενα παραδείγματα εδώ - πηγή: https://blog.usecure.io/the-most-common-examples-of-a-phishing-email#Email-account-upgrade-scam) • Πίνακας και μαρκαδόροι

Προετοιμασία	Κατά την προετοιμασία αυτού του μαθήματος, οι συντονιστές θα πρέπει να κάνουν τις παρακάτω ενέργειες: - Ανασκόπηση του σχεδίου μαθήματος - Εκτύπωση παραδειγμάτων phishing
Εφαρμογή	***Σχετική ορολογία:*** *Οι ακόλουθοι όροι θα συζητηθούν κατά τη διάρκεια του μαθήματος:* *- **Κωδικός πρόσβασης**: ένας συνδυασμός γραμμάτων, αριθμών και χαρακτηριστικών που πρέπει να εισαχθεί για να αποκτήσει κάποιος πρόσβαση σε πολλές διαδικτυακές υπηρεσίες (e-mail, λογαριασμοί κοινωνικών μέσων, λογαριασμοί ηλεκτρονικών αγορών κ.λπ.).* *- **Phishing**: η δόλια προσπάθεια απόκτησης ευαίσθητων πληροφοριών, όπως ονόματα χρηστών, κωδικοί πρόσβασης και στοιχεία πιστωτικών καρτών, μέσω της μεταμφίεσης σε μια αξιόπιστη οντότητα σε μια ηλεκτρονική επικοινωνία. Πολλές φορές, αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου ή τα μηνύματα κειμένου εμφανίζονται σαν να προέρχονται από νόμιμη πηγή και συνήθως έχουν την αίσθηση του επείγοντος. Οι σύνδεσμοι στα μηνύματα ηλεκτρονικού ταχυδρομείου phishing συνήθως οδηγούν τον χρήστη σε έναν μη αξιόπιστο ιστότοπο για την εισαγωγή ευαίσθητων πληροφοριών. Οι κίνδυνοι που σχετίζονται με τις απόπειρες phishing περιλαμβάνουν άτομα που αποκτούν τους κωδικούς πρόσβασής σας, που σας υποδύονται για να αποκτήσουν πρόσβαση στον τραπεζικό σας λογαριασμό και σε άλλες οικονομικές υπηρεσίες, που αγοράζουν αντικείμενα στο διαδίκτυο, άτομα που σας υποδύονται σε ιστότοπους κοινωνικής δικτύωσης και που έχουν πρόσβαση σε ιδιωτικές πληροφορίες στον υπολογιστή σας.* ***Δραστηριότητα 1: Τι είναι το Phishing;*** *Διανείμετε παραδείγματα phishing.* ***Εργασία σε ομάδες** (20 λεπτά) - χωρίστε τους μαθητές σε μικρές ομάδες των 4 μαθητών και δώστε τους παραδείγματα phishing (βλ. παράρτημα). Οι μαθητές έχουν το καθήκον να περιγράψουν τα επιμέρους παραδείγματα, αν πρόκειται για απάτη ή όχι. Εάν ναι, γιατί;* ***Παρουσίαση των αποτελεσμάτων των μαθητών** - (20 λεπτά)* ***Διευκρινίσεις και επεξηγήσεις** - (10 λεπτά)* ***Δραστηριότητα 2: Αντιμετώπιση προσπαθειών ηλεκτρονικού «ψαρέματος***

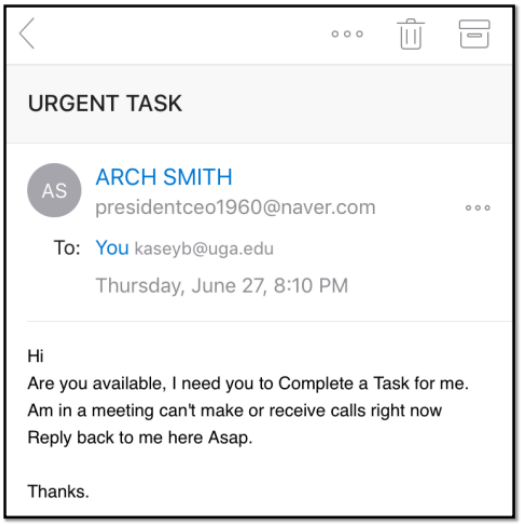
	Εισαγωγή/αφήγηση**: Γιατί είναι σημαντικό να αποφεύγονται οι απόπειρες ηλεκτρονικού «ψαρέματος»; Για παράδειγμα, ένας υπάλληλος στον δήμο μιας πόλης έδωσε άθελά του πρόσβαση σε τραπεζικά στοιχεία και ένας κυβερνοεγκληματίας κατάφερε να μεταφέρει σχεδόν 800.000 Ευρώ από τον λογαριασμό πριν κάποιος αντιληφθεί το λάθος. Παρόλο που η πόλη έχει ασφάλεια και η απάτη καταγγέλθηκε στις αρχές, είναι αδύνατον να ανακτηθούν τα χρήματα. Αν και το παράδειγμα αυτό αφορά μια πόλη, ο καθένας μπορεί να πέσει θύμα μιας απόπειρας ηλεκτρονικού «ψαρέματος».* ***Χρησιμοποιήστε ένα πίνακα και τους μαρκαδόρους για να κάνετε συλλογικό καταιγισμό ιδεών για τις ενέργειες που πρέπει να κάνετε σε περίπτωση που αντιμετωπίσετε μια απόπειρα ηλεκτρονικού ψαρέματος**. (10 λεπτά)* *Τα παραδείγματα περιλαμβάνουν:* *- Να μην κάνετε κλικ σε συνδέσμους ή να μην κατεβάζετε συνημμένα αρχεία. Μπορεί να περιέχουν ιούς ή λογισμικό κατασκοπείας.* *- Μην απαντάτε στο ηλεκτρονικό μήνυμα ή στο γραπτό μήνυμα.* *- Σημειώστε/κατηγοριοποιήστε το μήνυμα ηλεκτρονικού ταχυδρομείου ως «ανεπιθύμητο» ή «spam».* *- Εάν το μήνυμα ηλεκτρονικού ταχυδρομείου παραπέμπει σε έναν λογαριασμό και ανησυχείτε για τον λογαριασμό αυτό, καλέστε την εταιρεία. Ωστόσο, μην χρησιμοποιήσετε κανένα από τα στοιχεία επικοινωνίας στο μήνυμα ηλεκτρονικού ταχυδρομείου ή στο γραπτό μήνυμα. Πολλές φορές, αυτοί οι εγκληματίες δημιουργούν ψεύτικους τηλεφωνικούς αριθμούς. Επαληθεύστε πρώτα τα στοιχεία επικοινωνίας της εταιρείας αλλού.* *- Αναφέρετε το ηλεκτρονικό μήνυμα ηλεκτρονικού «ψαρέματος» στους αρμόδιους.* ***Δραστηριότητα 3: Εντοπίστε τις απόπειρες phishing *Κουίζ για την επαλήθευση των γνώσεων - (10 λεπτά) μπορείτε να το εκτελέσετε για όλους, κάθε μαθητής μπορεί να το κάνει ξεχωριστά και στη συνέχεια να μοιραστείτε τα αποτελέσματα μαζί.* *Αν και η πρόθεση είναι η δραστηριότητα να αναπτύξει δεξιότητες προστασίας της ιδιωτικής ζωής και ασφάλειας που σχετίζονται με την τεχνολογία, είναι σημαντικό ο συντονιστής να ηγηθεί μιας συζήτησης απολογισμού στο τέλος του μαθήματος. Πιθανές ερωτήσεις για τον απολογισμό θα μπορούσαν να περιλαμβάνουν:* *- Ποια είναι ορισμένα χαρακτηριστικά των αξιόπιστων ηλεκτρονικών επικοινωνιών;*

	- Ποια είναι ορισμένα χαρακτηριστικά των δόλιων ηλεκτρονικών επικοινωνιών; *- Γιατί είναι σημαντικό να γνωρίζετε πώς να αποφεύγετε τις απόπειρες ηλεκτρονικού «ψαρέματος»;* *- Τι πρέπει να κάνετε αν λάβετε ένα ηλεκτρονικό μήνυμα ή ένα μήνυμα που νομίζετε ότι είναι δόλιο;*
Συμβουλές	Συνιστούμε να κάνετε τεστ phishing με τους μαθητές στο τέλος του μαθήματος. Είναι ένας πολύ καλός προβληματισμός σχετικά με τις αποκτηθείσες γνώσεις. Διαθέσιμοι σύνδεσμοι: https://phishingquiz.withgoogle.com/. https://www.proprofs.com/quiz-school/topic/phishing
Μέτρα Ασφαλείας	-
Εξωτερικές αναφορές και πηγές	• https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams •https://www.commonsense.org/education/digital-citizenship/lesson/dont-feed-the-phish • https://georgia4h.org/wp-content/uploads/Something-is-Phishy.pdf
Συνεργάτες/ Συγγραφείς	CPM- Κέντρο πρόληψης Mladeze, Σλοβακία

Παράρτημα

Διανείμετε παραδείγματα ηλεκτρονικού μηνύματος και κειμένου phishing.

Παράδειγμα 1



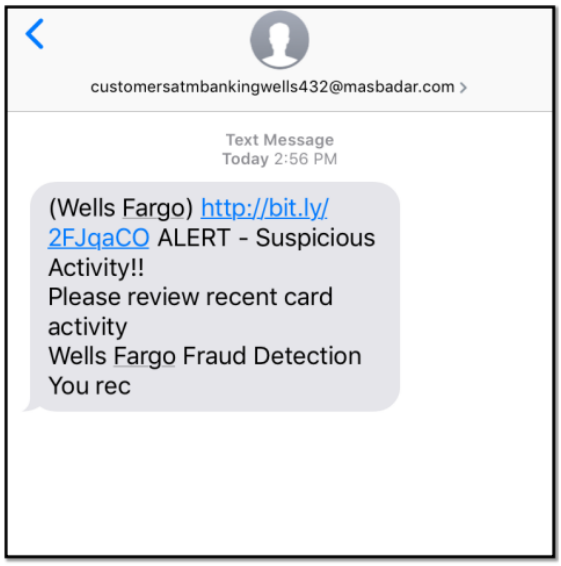
Μετά την άσκηση, εξηγήστε τα ακόλουθα για το μήνυμα κειμένου:

Ο υπάλληλος (που εργάζεται για το Πανεπιστήμιο της Τζόρτζια) έλαβε αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου. Ο προϊστάμενός της είναι ο Arch Smith, οπότε λαμβάνει τακτικά μηνύματα ηλεκτρονικού ταχυδρομείου από αυτόν. Ωστόσο, μετά από περαιτέρω έρευνα, υπάρχουν κάποια ύποπτα πράγματα σε αυτό το μήνυμα:

- Ενώ το μήνυμα ηλεκτρονικού ταχυδρομείου είναι από τον «Arch Smith», η διεύθυνση ηλεκτρονικού ταχυδρομείου που στάλθηκε δεν δείχνει ότι ο Arch έστειλε το μήνυμα. Δεδομένου ότι η αλληλογραφία σχετίζεται με την εργασία, είναι επίσης ύποπτο το γεγονός ότι δεν προέρχεται από λογαριασμό ηλεκτρονικού ταχυδρομείου που σχετίζεται με το Πανεπιστήμιο της Τζόρτζια.

- Η ορθογραφία, η γραμματική και η μηχανική του ηλεκτρονικού ταχυδρομείου προκαλούν ανησυχίες. Χρησιμοποιούνται λέξεις με κεφαλαία γράμματα που δεν θα έπρεπε. Η στίξη και η γραμματική είναι λανθασμένες σε ορισμένες περιπτώσεις.

Παράδειγμα 2



Μετά την άσκηση, εξηγήστε τα ακόλουθα για το μήνυμα κειμένου:

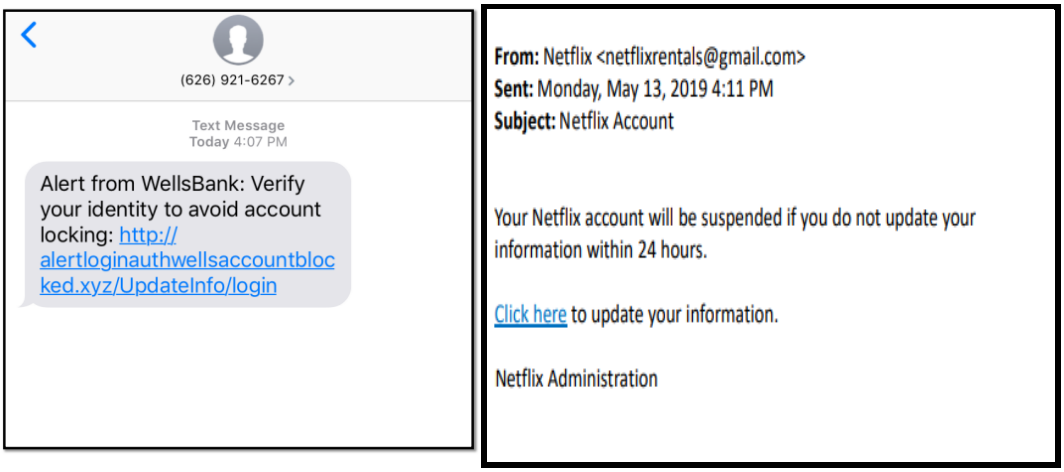
Το άτομο έχει τραπεζικές συναλλαγές με την Wells Fargo και μερικές φορές λαμβάνει ενημερώσεις μέσω ηλεκτρονικού ταχυδρομείου από την τράπεζα. Ωστόσο, μετά από περαιτέρω έρευνα, υπάρχουν κάποια ύποπτα πράγματα σε αυτό το μήνυμα:

- Ο αποστολέας αυτού του μηνύματος χρησιμοποιεί τη διεύθυνση ηλεκτρονικού ταχυδρομείου customersatmbankingwells432@masbadar.com. Δεν φαίνεται να είναι νόμιμη διεύθυνση ηλεκτρονικού ταχυδρομείου που σχετίζεται με την Wells Fargo.

- Ο σύνδεσμος που ενσωματώνεται στο μήνυμα είναι ένα μεγάλο url. Το Bigly είναι μια υπηρεσία που συντομεύει τα url - χωρίς να εμφανίζει το πλήρες url του ιστότοπου. Ενώ πολλές ομάδες χρησιμοποιούν αυτές τις υπηρεσίες, θα πρέπει να κάνετε κλικ στο συντομευμένο url μόνο όταν γνωρίζετε τον αποστολέα.

- Η σύνταξη και η γραμματική κειμένου προκαλούν ανησυχίες. Το μήνυμα δεν είναι πλήρες.

Παράδειγμα 3



Μετά την άσκηση, εξηγήστε τα ακόλουθα για το μήνυμα κειμένου:

Μια τυπική περίπτωση απόκτησης των δεδομένων της ηλεκτρονικής σας τραπεζικής - Πολλές φορές, οι άνθρωποι που απαντούν σε τέτοιου είδους μηνύματα ηλεκτρονικού ταχυδρομείου, κάνουν κάτι που δεν τους κρατάει ασφαλείς στο διαδίκτυο. Μπορεί επίσης να τους ζητηθεί να κάνουν κλικ σε έναν σύνδεσμο και να μοιραστούν πληροφορίες. Για παράδειγμα, μπορεί να τους ζητηθεί να μοιραστούν τον κωδικό πρόσβασής τους, οικονομικές πληροφορίες, κωδικούς pin ή να τους ζητηθεί να στείλουν χρήματα ή να αγοράσουν αντικείμενα (όπως δωροκάρτες). Πολλές φορές, η χρονική στιγμή είναι επείγουσα επειδή «εντοπίστηκε ύποπτη δραστηριότητα» ή «ο λογαριασμός σας έχει κλειδωθεί» μέχρι να γίνουν περαιτέρω ενέργειες.

Ορισμένα χαρακτηριστικά ενός ηλεκτρονικού μηνύματος «ψαρέματος» περιλαμβάνουν:

- **Ανάγκη επαλήθευσης πληροφοριών** λογαριασμού (π.χ. λογαριασμός ηλεκτρονικού ταχυδρομείου, τραπεζικός λογαριασμός, λογαριασμός μεταφοράς χρημάτων κ.λπ.) Πολλές φορές, το μήνυμα ηλεκτρονικού ταχυδρομείου αναφέρει ότι οι προσωπικές σας πληροφορίες έχουν λήξει ή πρέπει να επαληθευτούν.

- **Σύνδεσμος στο μήνυμα ηλεκτρονικού ταχυδρομείου/κείμενο ή στο συνημμένο αρχείο**. Συνήθως, ο σύνδεσμος δεν σας παρέχει τη διεύθυνση URL, οπότε είναι δύσκολο να προσδιορίσετε σε ποιον ιστότοπο θα σας ανακατευθύνει. Ανεξάρτητα από αυτό, κάντε κλικ μόνο σε συνδέσμους από αξιόπιστους αποστολείς.

- **Αίσθηση επείγοντος**. Πολλές φορές, τα μηνύματα ηλεκτρονικού ταχυδρομείου phishing σας δίνουν ένα περιορισμένο χρονικό διάστημα (π.χ. 24 ώρες) για να επιλύσετε ένα «πρόβλημα» που δεν υπάρχει.

- **Πολύ καλό για να είναι αληθινό**. Τα μηνύματα ηλεκτρονικού ταχυδρομείου phishing μπορεί να υπόσχονται κάποιο είδος «ανταπόδοσης», όπως μετρητά ή δωροκάρτες, αν κάνετε πρώτα κάτι (συνήθως δίνοντάς τους προσωπικές/ευαίσθητες πληροφορίες).

- **Ορθογραφικά, γραμματικά ή/και συντακτικά λάθη.** Ένα περιστασιακό τυπογραφικό λάθος συμβαίνει μερικές φορές σε ένα νόμιμο μήνυμα ηλεκτρονικού ταχυδρομείου, αλλά ένα μήνυμα ηλεκτρονικού ταχυδρομείου phishing περιλαμβάνει συνήθως σημαντικό αριθμό λαθών.

- **Μήκος.** Ορισμένα μηνύματα ηλεκτρονικού ταχυδρομείου phishing μπορεί να τείνουν να είναι σύντομα. Άλλα μπορεί να είναι πολύ μεγάλα, εξηγώντας μια περίσταση (π.χ. γιατί αυτό το άτομο δεν μπορεί να κάνει κάτι και γιατί χρειάζεται τη βοήθειά σας).

- **Γενικός χαιρετισμός.** Πολλά μηνύματα ηλεκτρονικού ταχυδρομείου ηλεκτρονικού «ψαρέματος» δεν έχουν χαιρετισμό ή απλά ξεκινούν με «γεια σας».

Conscious Youth Behaviours in Emerging Realities

Erasmus+ KA2 Cooperation Partnerships in School Education

[Reference n. 2023-1-EL01-KA220-SCH-000156982]

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.