Project no: 2020-1-LT01-KA203-078070

“ΑΝΑΓΝΩΡΙΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΨΑΡΕΜΑΤΟΣ ΚΑΙ ΤΟΥ ΧΑΣΜΑΤΟΣ ΤΩΝ ΔΕΞΙΟΤΗΤΩΝ ΠΑΝΩ ΣΕ ΑΥΤΟ”

ΠΑΡΟΥΣΙΑΣΗ

2021

Συνεργασία

Vilnius University, Lithuania

Website: http://www.vu.lt

University of Tartu

Website: https://www.ut.ee/et

MECB - Macdac Engineering Consultancy Bureau LTD , Malta

Website: http://www.mecb.com.mt/eu

Altacom SIA, Latvia

Website: https://www.altacom.eu/

DOREA Educational Institute, Cyprus

Website: https://dorea.org/

ECDL- Information Technologies Institute, Lithuania

Website: http://www.ecdl.lt/

Funded by the Erasmus+ Programme of the European Union

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ 6

1.1. Ηλεκτρονική ασφάλεια στην ΕΕ: πραγματικότητα και ανάγκες 6

1.2. "Προστασία κατά του ηλεκτρονικού ψαρέματος στην εποχή της 4ης Βιομηχανικής Επανάστασης" πρότζεκτ 8

2. ΗΛΕΚΤΡΟΝΙΚΌ "ΨΆΡΕΜΑ" 10

2.1. Τί είναι το ηλεκτρονικό "ψάρεμα" ; 10

2.2. Κοινωνική μηχανική και ηλεκτρονικό ψάρεμα 11

2.3. Ηλεκτρονικό ψάρεμα κατά τη διάρκεια του COVID-19 14

3. ΈΡΕΥΝΑ ΓΙΑ ΜΑΘΗΤΕΣ, ΥΠΑΛΛΗΛΟΥΣ ΚΑΙ ΔΙΕΥΘΥΝ ΣΥΜΒΟΥΛΟΥΣ 16

3.1. Η μεθοδολογία της συλλογής δεδομένων 16

3.2. Συλλογή Αποτελεσμάτων 17

3.3. Αποτελέσματα και ανάλυση των ερευνών 18

3.3.1. Επισκόπηση των ερωτηθέντων 18

3.3.2. Γενικές γνώσεις και συμπεριφορές 19

3.3.3. Προσωπική εμπειρία με τις επιθέσεις ηλεκτρονικού ψαρέματος 24

3.3.4. Αναγνώριση των επιθέσεων ηλεκτρονικού ψαρέματος 25

3.3.5. Δεξιότητες κριτικής σκέψης 29

3.3.6. Αποφυγή επιθέσεων ηλεκτρονικού ψαρέματος 30

4. ΣΥΝΟΨΗ ΚΑΙ ΚΥΡΙΑ ΠΟΡΙΣΜΑΤΑ 33

5. ΒΙΒΛΙΟΓΡΑΦΙΑ 38

Παράρτημα 1. Έρευνα "Αξιολόγηση των δεξιοτήτων και ανανγώριση των διαδικτυακων/phishing επιθέσεων" 39

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Λίστα Πινάκων

Table 1. Αριθμός ερωτηθέντων ανα χώρα. 18
Table 2. Ερωτηθέντες ανα γένος 18
Table 3. Τρόποι που έπεσαν θύματα ηλεκτρονικού ψαρέματος οι ερωτηθέντες στο παρελθόν. 24
Table 4. Λόγοι γιατί πιστεύουν οι ερωτηθέντες οτι έπεσαν θύματα ηλεκτρονικού ψαρέματος 25
Table 5. Τα περισσότερο και λιγότερο σημαντικά κριτήρια για την αναγνώριση επιθέσεων ηλεκτρονικού ψαρέματος 28

Λίστα Περιεχομένων

Figure 1. Έρευνα της κατάστασης απασχόλησης των ερωτηθέντων 19
Figure 2. Έρευνα του επιπέδου εκπαίδευσης των ερωτηθέντων 19
Figure 3. Έρευνα της επίγνωσης των ερωτηθέντων σχετικά με το ηλεκτρονικό ψάρεμα 20
Figure 4. Οι τύποι των ηλεκτρονικού "ψαρέματος" που γνωρίζουν περισσότερο οι ερωτηθέντες 21
Figure 5. Τύποι ηλεκτρονικού ψαρέματος που γνωρίζουν λιγότερο οι ερωτηθέντες 21
Figure 6. Συνέπειες που είναι πιθανότερο να επιτευχθούν μετά απο μία ηλεκτρονική επίθεση σύμφωνα με τους ερωτηθέντες 22
Figure 7. Τύποι email που είναι πιθανότερο οι ερωτηθέντες να κλικάρουν στον σύνδεσμο ή στο συννημένο αρχείο μέσα στο email ή το μήνυμα ή/και να παρέχουν ευαίσθητες πληροφορίες 22
Figure 8. Τύποι μηνυμάτων ηλεκτρονικού ταχυδρομείου που είναι λιγότερο πιθανό να κλικάρουν στο σύνδεσμο ή στο συνημμένο αρχείο στο email ή στο μήνυμα ή/και να παρέχουν ευαίσθητες πληροφορίες οι ερωτηθέντες. 23
Figure 9. Εστίαση και προσοχή των ερωτηθέντων στις λεπτομέρειες κατά το άνοιγμα ενός μηνύματος/email 29
Figure 10. Τα επίπεδα προσοχής των ερωτηθέντων όταν κάνουν κλικ σε έναν σύνδεσμο/ συνημμένο αρχείο. 29
Figure 11. Κύριοι λόγοι που οι επιθέσεις ηλεκτρονικού ψαρέματος είναι επιτυχείς σύμφωνα με τους ερωτηθέντες. 30
Figure 12. Ενέργειες που πρέπει να ληφθούν για την πρόληψη επιθέσεων ηλεκτρονικού ψαρέματος σύμφωνα με τους ερωτηθέντες 31

Funded by the Erasmus+ Programme of the European Union

Figure 13. Περιοχές στις οποίες οι ερωτηθέντες νιώθουν περισσότερη αυτοπεποίθηση 32

Λίστα Συντομεύσεων

CEO	Διευθύνων Σύμβουλος
ENISA	Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών
EU	Ευρωπαϊκή Ένωση
EUROPOL	Η υπηρεσία πληροφοριών σε ζητήματα εγκληματικής φύσης της Ευρωπαϊκής Ένωσης

Funded by the Erasmus+ Programme of the European Union

1. ΕΙΣΑΓΩΓΗ

1.1. Ηλεκτρονική ασφάλεια στην ΕΕ: πραγματικότητα και ανάγκες

Η Ευρωπαϊκή Επιτροπή προετοίμασε και διεξήγαγε μια ειδική Ευρωβαρομετρική έρευνα το 2019 με στόχο τις γνώσεις, τις εμπειρίες και τις αντιλήψεις των Ευρωπαίων Πολιτών πάνω στο θέμα της ηλεκτρονικής ασφάλειας.

Όπως ήταν αναμενόμενο, τα αποτελέσματα έδειξαν ότι η χρήση του ίντερνετ συνεχίζει να αυξάνεται στην Ευρώπη, συγκεκριμένα μεσω κινητού. Τα αποτελέσματα επίσης έδειξαν οτι οι Ευρωπαίει Πολίτες είναι πιο προσεκτικοί με του πιθανούς κινδύνους του να συνδεθούν και να χρησιμοποιούν το ίντερνετ, με 52% των ερωτηθέντων να δηλώνουν οτι είναι αρκετά καλα ή πολύ καλά ενημερωμένοι στο θέμα του ηλεκτρονικού εγκλήματος, σε σχέση με το ποσοστό 46% που υπερέιχε το 2017. Σύμφωνα με τα πορίσματα της έρευνας, οι ανησυχίες που αφορούν το διαδικτυακό απόρρητο και την διαδικτυακή ασφάλεια έχουν ήδη οδηγήσει 9 στους 10 χρήστες του Ίντερνετ να αλλάξουν την συμπεριφορά τους- συχνότερα να μην ανοίγουν email απο άγνωστους ανθρώπους, να εγκαθιστούν πρόγραμμα για την καταπολέμηση των ιών του υπολογιστή, να επισκέφτονται ιστοσελίδες που ξέρουν και εμπιστεύονται και να συνδέονται μονο απο τους δικούς τους υπολογιστές[1].

Όσο και αν αυτα τα αποτελέσματα ειναι ενθαρρυντικά, απο την άλλη μεριά πολλοί χρήστες του Ίντερνετ γίνανται θύματα διαδικτυακής απάτης και δολώματα σε phishing emails. Σύμφωνα με τα στοιχεία της Ευρωστατ, το 2019, περίπου 1 στους 3 Ευρωπαίους πολίτες ηλικίας 16 με 74 ανέφερε περιστατικο που σχετίζεται με την ασφάλεια καθώς χρησιμοποιεί το Ίντερνετ για προσωπικύς λόγους το 2019 μέσα στους τελευταίους 12 μήνες.

Κατά την διάρκεια αυτής της περιόδου - το phishing ήταν το συχνότερο περιστατικό ασφάλειας που αναφέρθηκε το 2019. 25% των ερωτηθέντων δήλωσαν οτι έλαβαν μηνύματα εξαπάτησης, γνωστά και ως phishing, ενώ το 12% των ερωτηθέντων δήλωσαν οτι καθοδηγούνται σε ψεύτικες ιστοσελίδες στις οποίες τους ζηταύνται να δώσουν προσωπικές πληροφορίες τους (pharming)

Τα υψηλότερα ποσοστά παρατηρήθηκαν στη Δανία (50%), ακολουθούμενη από τη Γαλλία (46%), τη Σουηδία (45%), τη Μάλτα και τις Κάτω Χώρες (και οι δύο 42%), τη Φινλανδία (41%) και τη Γερμανία (40%). Αντίθετα, τα χαμηλότερα ποσοστά καταγράφηκαν στη Λιθουανία (7%), στην Πολωνία (9%), στη Λετονία (10%), στη Βουλγαρία (13%) και στην Ελλάδα (13%).

[1] European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020

Funded by the Erasmus+ Programme of the European Union

Το ποσοστό των ατόμων που αντιμετωπίζουν προβλήματα που σχετίζονται με την ασφάλεια είναι στην Εσθονία και την Κύπρο ήταν 32% και 21% αντίστοιχα[2].

Το μερίδιο των ανθρώπων το οποίο εχει βιωσει περιστατικο που να σχετίζεται με την ασφάλεια χρησιμοποιόντας το Ίντερνετ για προσωπικούς λόγους ποικίλει μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης.

Αυτό μπορεί να εξηγηθεί απο τις διαφορές ανάμεσα στο επίπεδο ευαισθητοποίησης του διαδικτυακού εγκλήματος μεταξυ των χωρών της ΕΕ*, η γενική μείωση εμπιστοσύνης των πολιτών της ΕΕ του να είναι σε θέση να προστατέψουν τους εαυτούς τους απο διαδικτυακές επιθέσεις, καθώς και οι διαδικτυακές επιθέσεις γίνονται πιο εκλεπτυσμένες πραγμα που τις κανει να είναι δυσκολότερο να τις εντοπίσεις και να τις αποφύγεις, νέες τεχνικές χρησιμοποιούνται και νέες πλατφορμες ειναι διαθέσιμες για να πραγματοποιούνται τέτοιες επιθέσεις.

Όσο αναφορά τον επαγγελματικό τομέα στην Ευρώπη, είναι και αυτος, επηρεασμένος απο θέματα διαδικτυακής ασφάλειας. Οι Ευρωπαικές χώρες και επιχειρήσεις στοχοποιούνται λογω της συχνότητας ανάπτυξής τους. Σύμφωνα με την Παγκόσμια έρευνα για την ασφάλεια πληροφοριών, περίπου το 80% των εταιρειών της Ευρώπης έχουν βιώσει τουλάχιστον μία φορά περιστατικό διαδικτυακής ασφάλειας μέσα σε αυτή τη χρονία και οι υπάλληλοι είναι υπεύθυνοι για το 27% αυτών των περιστατικών.

Παγκοσμίως, βάση πρόσφατων στοιχείων, στο πρώτο τρίμηνο του 2019, οι εταιρείες στοχοποιήθηκαν 120% περισσοτερα απο οτι ένα χρόνο πριν, με αποτέλεσμα να υπάρχει ζημία που να ανέρχεται στο ποσό των 22,2 δισεκατομμυρίων ευρώ €.

Περισσότερο από το 99% των e-mail που διανέμουν κακόβουλο λογισμικό απαιτούν ανθρώπινη παρέμβαση με - την ακολούθηση συνδέσμων, το άνοιγμα εγγράφωμ, την αποδοχή προειδοποιήσεων ασφαλείας και άλλες τέτοιες συμπεριφορές - ώστε να είναι αποτελεσματικά.[3]

Συνεπώς, οι άνθρωποι, είτε είναι στη δουλειά τους είτε στο σπίτι τους, οι οποίοι ειναι ενημερωμένοι για τα προειδοποιητικά σημάδια και έχουν τη γνώση των σωστών τεχνικών, ειναι τα βασικά στοιχεία για να επιβραδυνθούν ή να αποτρέψουν τις διαδικτυακές επιθέσεις. Επομένως, υπάρχει η ανάγκη για ενημέρωση των ήδη υπάρχοντων προγραμμάτων διαδικτυακής ασφάλειας ή η δημιουργία καινούργιων για την βελτίωση των δεξιοτήτων, της

[2] EUROSTAT (2020): Is internet use safer today?, URL https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb/default/table?lang=en (accessed 11.02.2021)

[3] Proofpoint (2019): Human Factor Report 2019, URL https://www.proofpoint.com/us/resources/threat-reports/human-factor (accessed 12.02.2021)

Funded by the Erasmus+ Programme of the European Union

εκπαίδευσης και των γνωσεων των πολιτών της ΕΕ στα τελευταία αναδυόμενα ζητήματα και απειλές που αφορούν την διαδικτυακή ασφάλεια.

Υπάρχει επίσης η ανάγκη να προσφέρονται τέτοια προγρράμματα σε όλους τους μαθητές, αναλογιζόμενοι οτι σύμφωνα με την ENISA, στα πανεπιστήμια, θέματα που σχετιζονται με το διαδίκτυο υποεκπροσωπούνται σε μη τεχνικά προγράμματα.

1.2. "Προστασία κατά του ηλεκτρονικού ψαρέματος στην εποχή της 4ης Βιομηχανικής Επανάστασης" πρότζεκτ

Η διαδικτυακή ασφάλεια γένται μια απο τις μεγαλύτερες προκλήσεις της ψηφιακής εποχής, διότι οι πληροφορίες καθίστανται ενα ακριβό προσόν που ασχολείται με έναν τεράστιο όγκο δεδομένων, βελτιώνοντας την επικοινωνία με το ψηφιακό περιβάλλον. Οι ψηφιακές συσκευές και τα συστήματα επικοινωνίας γίνονται ολο και περισσότερο ελκυστικά για διαδικτυακές επιθέσεις.

Το phishing είναι ένα απο τα μεγαλύτερα προβλήματα διότι οι διαδικτυακοί εγκληματίες μπορούν να χρησιμοποιούν γρηγορότερα και να καινοτομούν τεχνολογικά εργαλεία για να διεξάγουν phishing εκστρατείες. Συνεπώς το ανθρώπινο αμυντικό συστημα το οποίο μοχλεύει το ανθρώπινο ένστικτο για την ανακάλυψη και την τεχνολογία ώστε να κλιμακώσει την απόκριση αυτή θα μπορούσε να αναπτυχθεί και να είναι ελεύθερα διαθέσιμο για το ευρύ κοινό. Για τη δημιοργία ενός ανθρώπινου αμυντικού συστήματος, απαιτείται εκπαίδευση του χρήστη ώστε να είναι ικανός να αναγνωρίσει και να ανταποκριθεί στις επιθέσεις phishing με τον σωστό τρόπο.

Η Διεθνής μελέτη "Safeguarding against Phishing in the age of 4 Industrial Revolution" („CyberPhish") που ξεκίνησε απο το Πανεπιστήμιο του Βίλνιους της σχολής Καούνας και των συνεργατών της ξεκίνησαν στις αρχές του Νοεμβρίου του 2020 και θα διαρκέσουν για 2 χρόνια.

Ο στόχος του πρότζεκτ ειναι να εκπαιδείσει: μαθητες απο ανώτερα εκπαιδευτικά ιδρύματα, τους ίδους τους εκπαιδευτες, πανεπιστημιακό προσωπικό (μέλη της κοινότητας), άλλα εκπαιδευτικά κέντρα, επαγγελματικους τομεις (εργοδότες και εργαζομένους), και να εθαρυνει την κριτική σκέψη αυτών των ομάδων στο πεδίο της διαδικτυακής ασφάλειας.

Οι συνέταιροι του προτζεκτ πρεπει να σχεδιάσουν ενα πρόγραμμα μαθημάτων, υλικό ηλεκτρονικής μάθησης, ενα συνδυαστικό μαθησιακό περιβάλλον, οπου γνώσεις και αυτοαξιολόγηση ικανοτήτων και προσομοιώσεις συστημάτων αξιολόγησης γνώσεων για μαθητές και άλλους χρήστες ώστε να αποτρέψουν επιθέσεις phishing, να αυξήσουν τις

Funded by the Erasmus+ Programme of the European Union

ικανότητές τους, οι οποίες θα τους βοηθήσουν να επικεντρώσουν την προσοχή τους στις απειλές και να λάβουν τα κατλληλα μέτρα για να εμποδίσουν αυτες τις επιθέσεις.

Η συνεργασία του έργου αυτού προέρχεται απο 6 οργανισμούς οι οποίοι προέρχονται απο 5 διαφορετικές χώρες:

1. Vilnius University, Lithuania (Coordinator)
2. Information Technologies Institute, Lithuania
3. DOREA Educational Institute, Cyprus
4. Tartu Ulikool, Estonia
5. Altacom SIA, Latvia
6. Macdac Engineering Consultancy Bureau Ltd (MECB), Malta

Για περισσότερες πληροφορίες οσο αναφορά το πρότζεκτ και τις δραστηριότητες αυτου, παρακαλώ επισκεφθείτε την ιστοσελίδα του πρότζεκτ: https://cyberphish.eu/

Funded by the Erasmus+ Programme of the European Union

2. ΗΛΕΚΤΡΟΝΙΚΌ “ΨΆΡΕΜΑ”

2.1. Τί είναι το ηλεκτρονικό “ψάρεμα” ;

Το phishing είναι μία απόπειρα απάτης για να κλέψει κάποιος δεδομένα απο κάποιον χρήστη του ίντερνετ όπως διαπιστευτήρια σύνδεσης σε μια ιστοσελίδα, πληροφορίες της πιστωτικής κάρτας, η ακόμη και χρήματα χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής. Αυτού του είδους η επίθεση συνήθως πραγματοποιείται μέσω email, που φαίνεται να προέρχονται απο μία αξιόπιστη πηγή, με την πρόθεση να πείσουν τον χρήστη να ανοίξει ένα κακόβουλο συνημμένο αρχείο ή να ακολουθήσει μία ψεύτικη ιστοσελίδα[4].

Το phishing είναι μία απο τις παλαιότερες διαδικτυακές επιθέσεις, χρονολογείται απο το 1990. Παρόλο που υπάρχει για δεκαετίες, είναι ακόμη ενα απο τα πιο διαδεδομένα και καταστροφικά είδη διαδικτυακής επίθεσης[5].

Υπάρχουν πολλά είδη phishing, όμως τα πιο συνηθισμένα είναι:

1) *Spray and pray* – κακόβουλα email τα οποία στέλνονται σε οποιαδήποτε διεύθυνση ηλεκτρονικού ταχυδρομείου ώστε να κλέψουν ευαίσθητες πληροφορίες
2) *Spear fishing* - κακόβουλα email τα οποία δημιουεργούνται και στέλνονται σε συγκεκριμένα άτομα ή οργανισμούς ώστε να κλέψουν ευαίσθητες πληροφορίες
3) *Whaling* - η προσπάθεια να κλέψουν ευαίσθητες πληροφορίες και συνήθως στοχοποιείται το διοικητικό προσωπικό
4) *Vishing* - αναφέρεται στην απάτη του phishing που πραγματοποιείται μέσω του τηλεφώνου
5) *Smishing* - αναφέρεται στο phishing με μηνύματα SMS, αντί για email, που στοχοποιούν ενα άτομο
6) *Angler Phishing* – σχετικά καινούργιου τύπου απατη, η οποία αναφέρεται σε επιθέσεις οι οποίες υπάρχουν στα μέσα κοινωνικής δικτύωσης χρησιμοποιώντας ψεύτικες ιστοσελίδες, κλωνοποιημένους ιστοτόπους, όπως και tweets για άμεσα μηνύματα.
7) *Clone Phishing* - τύπος phishing οπου ενα έγκυρο email που έχει παραδοθεί παλαιότερα, χρησιμοποιείται ώστε να δημιουργηθεί ενα πανομοιότυπο email με κακόβουλο περιεχόμενο

[4] European Union Agency for Cybersecurity (2020): Phishing - ENISA threat landscape 2019-2020
[5] Deloitte (2019): Understanding Phishing Techniques URL https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf (accessed 112.02.2021)

Funded by the Erasmus+ Programme of the European Union

8) *Malvertising* - αυτού του τύπου phishing χρησιμοποιεί διαδικτυακές διαφημίσεις ή αναδυόμενα παράθυρα που εμφανίζονται ως διαφημίσεις ώστε να αναγκάσει τους ανθρώπους να πατήσουν/κλικάρουν έναν σύνδεσμο ο οποίος φαινεται έγκυρος, αλλά όμως εγκαθιστά κακόβουλο λογισμικό στον υπολογιστη

Η αυξανόμενη πολυπλοκότητα του phishing παρατηρήθηκε τα τελευταία 2 χρόνια, με το phishing να γίνεται όλο και πιο δύσκολα ανιχνεύσιμο, πολλά phishing email και ιστοσελίδες είναι σχεδόν πανομοιότυοπα με τα αληθινά. Την ίδια στιγμή, οι εκτρατείες του phishing έχουν γίνει γρηγορότερες και περισσότερο αυτοματοποιημένες ώστε να δρούν γρηγορότερα απο οτι πρίν και σε μερικές περιπτώσεις χριάζεται μόνο μία μέρα για να γίνει απο μία διαρροή διαπιστευτηρίου μία ολόκληρη επίθεση.

Σύμφωνα με την έρευνα της Ευρωπολ οι διαδικτυακοί εγκληματίες χρησιμοποιούν μια πιο ολοκληρωμένη στρατηγική πάνω στο phishing με το να δείχνουν ένα υψηλό επίπεδο ικανότητας όσο αναφορά στην χρησιμοποίηση των εργαλείων, συστημάτων και αδυναμιών που εκμεταλλεύονται, υποθέτωντας οτι έχουν ψευδής ταυτότητες και δουλεόντας σε συνεργασία με άλλους διαδικτυακούς εγκληματίες. [6]

Στο μέλλον, τα email προβλέπεται να συνεχίσουν να ειναι ο νούμερο ένα μηχανισμός του phishing, ωστόσο οχι για πολύ. Ειδικοί παρατηρούν μία αύξηση στην χρήση των μέσων κοινωνικής δικτύωσης με την μορφή μηνυμάτων, το WhatsApp και άλλα για να διεξάγουν τέτοιες επιθέσεις. Σύμφωνα με τον ENISA, η πιο σχετική αλλαγή θα είναι στις μεθόδους που χρησιμοποιούνται για να στείλουν τα μηνύματα, οι οποίες θα γίνουν περισσοτερο προωρημένου επιπέδου με την υιοθέτηση της ανταγωνιστικής τεχνητής νοημοσύνης να ετοιμάζει και να στέλνει μηνύματα.

2.2.Κοινωνική μηχανική και ηλεκτρονικό ψάρεμα

Στο πλαίσιο της ασφάλειας πληροφοριών, η κοινωνικλη μηχανική ορίζεται ως την ψυχολογική χειραγώγηση των ανθρώπων να εκτελούν ενέργειες ή να αποκαλύπτουν εμπιστευτικές πληροφορίες. Η κοινωνική μηχανική παραμένει μια κορυφαία απειλή που διευκολύνει άλλου τύπου διαδικτυακά εγκλήματα αφού το 84% των διαδικτυακών επιθέσεων βασίζονται στην κοινωνική μηχανική (ENISA). Ο αριθμός των ατόμων που έχουν πέσει θύματα phishing συνεχίζει να αυξάνεται αφού εκμεταλλεύται την ανθρώπινη διάσταση ως τον πιο αδύναμο σύνδεσμο.

[6] EUROPOL (2020): Internet Organised Crime Threat Assessment 2020

Funded by the Erasmus+ Programme of the European Union

Στοχοποιώντας την ανθρώπινη αδυναμία, η κοινωνική μηχανική και το phishing έχουν μεγάλη επίδραση στην κοινωνία και επιτρέπουν την πλειοψηφία των διαδικτυακών εγκλημάτων, που καλυπτουν όλο το φάσμα της απάτης μέχρι και την απόκτηση ευαίσθητων πληροφοριών και προχωρημώνων επιθέσεων μέσων κακόβουλων λογισμικλων.

Οι διαδικτυακοί εγκληματίες έχουν εκπαιδευτεί και έχουν γίνει άριστοι στην κοινωνική μηχανική, γίνονται ελκυστικοί απέναντι στην ανθρώπινη φύση ώστε να διάπραξουν την απάτη. Οι πιο συνηθισμένοι μέθοδοί τους που χειραγωγούν τους ανθρώπους που συνήθως βασίζονται σε αυτούς ειναι, ο φόβος, ο εκφοβισμος, η αίσθηση οτι υπάρχει επείγουσα ανάγκη, η απληστία, η περιέργει, η εκ φύσεως εμπιστοσύνη και η ενσυναίσθηση/συμπόνια. Οι διαδικτυακοί εγκληματίες γνωρίζουν οτι ειδικά σχεδιασμένα και προσωποπιημένα email, φωνητικά μηνύματα/ κλήσεις ή γραπτά μηνύματα μπορούν να παραπλανήσουν τους ανθρώπους να διαθέσουν ευαίσθητες πληροφορίες, να στείλουν χρήματα ή να κατεβάσουν το αρχείο που περιέχει κακόβουλο λογισμικό στο δίκτυο της εταιρείας.

Για να καταλάβουμε καλύτερα την κοινωνικλη μηχανική, μπορούμε να ρίξουμε μια ματιά στις 6 βασικές αρχές τις πειθούς , όπου ο Dr. Robert B. Cialdini εξήγησε στο βιβλίο του: “Influence: The Psychology of Persuasion” (= “Επιρροή: Η Ψυχολογία της Πειθούς”)[7]. Ενώ αρχικά αυτές οι αρχές χρησιμοποιόντουσαν στο μάρκετινγκ, υιοθετήθηκαν και χρησιμοποιήθηκαν εύκολα στην κοινωνική μηχανική όπως και στο phishing[8]:

1. Δοσοληψία - αυτό ειναι απλα το “πάρε και δώσε”/ “δούναι και λαβείν”. Ένα email προσφέρει μία έκπτωση ή κάποιο κουπόνι για κάποια ψώνια με αντάλλαγμα την κοινοποίηση πληροφοριών ή την εγγραφη σε κάποιον λογαριασμό; ένα email που υπόσχεται να δώσει πρόσβαση σε εμπιστευτικές πληροφορίες εάν ένα συγκεκριμένο αρχείο κατέβει στον υπολογιστή ή ένας σύνδεσμος πατηθεί/κλικαριστεί είναι τα κλασσικά παραδείγματα.
2. Έλλειψη/Ανεπάρκεια - είναι στην ανθρώπινη φύση να ζητάει ο άνθρωπος αυτό ειναι δύσκολο να αποκτήσει. Ένα phishing email που τονίζει οτι ένα συγκεκριμένο προνόμιο είναι προσβάσιμο μόνο εάν γίνει μία πράξη μέσα σε ένα σύντομο χρονικό διάστημα. “Ο λογαριασμίς θα απενεργοπιηθεί μέσα στις επόμενες 24 ώρες αν δεν πατήσετε/κλικάρετε αυτόν τον σύνδεσμο ώστε να μπορέσετε να επιλύσετε αυτό το πρόβλημα” είναι το παράδειγμα αυτής της αρχής.
3. Εξουσία - οι άνθρωποι τείνουν να ακολουθούν την εξοθσία και να πιστεύουν τους ειδικούς γενικότερα. Επομένως, πολλά phishing emails επιδιώκουν να μιμηθούν τις

[7] Dr Robert B. Cialdini is a Psychology and Marketing professor in the Arizona State University in USA
[8] NCC group (2020) :Psychology of the Phish: Leveraging the Seven Principles of Influence, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433 (accessed 12.02.2021)

Funded by the Erasmus+ Programme of the European Union

τοπικές αρχές, τους Διευθύνων Συμβούλους, τα ανώτερα στελέχη, του διευθυντές του ανθρώπινου δυναμικού, κλπ. Ένα email απο τον Διευθύνων Σύμβουλο (θεωρητικά) ζητάει απο το οικονομικό τμήμα να στείλει αμέσως ένα ποσό χρημάτων σε έναν λογαριασμό άγνωστο για την εταιρεία και το τμήμα αυτό, είναι ένα απο τα παραδείγματα προκύπτουν πολλές φορές.

4. Συνήθεια/συνέπεια - οι άνθρωποι είναι, με τον έναν ή τον άλλον τρόπο, δημιοθργήματα της συνήθειας. Τα phishing email που μοιάζουν ως επίσημα μηνύματα εκμεταλλεύονται αυτό το γεγονός, ελπίζωντας οτι ο παραλήπτης θα παραβλέψει το ασυνήθιστο αυτό αίτημα που είναι γραμμένο μέσα στο email. Ένα email με το λογότυπο της Amazon λέει οτι ένα φορτίο/δέμα έχει καθυστερήσει ζητάει τον παραλήπτη ώστε να επιβεβαιώσει την διεύθυνση κατοικίας μπορεί να μην κινήσει υποψίες ακόμη και αν δεν περιμένει κάποιος κάποιο φορτίο/δέμα - αυτή είναι η δύναμη μια ευρέως αναγνωρίσιμης μάρκας/φίρμας.
5. Επικρατούσα άποψη - οι άνθρωποι τείνουν να ακολουθούν άλλους ανθρώπους, ειδικά όταν δεν έιναι σίγουροι για κάτι. Ένα phishing email το οποίο αναφέρει οτι “544 στους 800 εργαζομένους έχουν ανβαθμίσει το λογισμικό τους, πατήστε/κλικάρετε τον σύνδεσμο για να το κατεβάσετε” εκμεταλλεύεται αυτήν την τάση.
6. Αρέσκεια/Συμπάθεια - αυτή ειναι αρκέτα απλή αρχή - αν είσαι αρεστός στους ανθρώπους ή αντιθέτως αν θέλεις να είσαι αρεστος πρός τους άλλους τότε είναι πιθανότερο να απαντήσουν με “ναι”. Ένα email απο το τμήτα IT της επιχείρησης (θεωρητικά) ζητήσει απο έναν νέο υπάλληλο τα προσωπικά του στοιχεία/ κωδικούς για να αναβαθμίσει το σύστημα προστασίας του είναι ένα παράδειγμα.
7. Ενότητα - αυτή η αρχή εντάχθηκε αργότερα. Η ιδέα πάνω σε αυτήν είναι οτι όσο περισσότερο ταυτίζουμε τους εαυτούς μας με άλλους, τόσο περισσότερο επηρεαζόμαστε απο αυτούς. Ένα phishing email έχει σταλεί θεωρητικά απο κάποιον που μοιράζεται τα ίδια ενδιαφέροντα με τον παραλήπτη του email, πληροφορίες που μπορούν εύκολα να βρεθούν/δωθούν μέσω των μέσων κοινωνικής δικτύωσης, έχουν μεγαλύτερο ποσοστό επιτυχίας. Για παράδειγμα, αν ένα άτομο αγαπάει τα σκυλιά, ένα email απο έναν άλλον λάτρη των σκυλιών (θεωρητικά) με ένα συνημμένο αρχείο ενός χαριτωμένου σκύλου (θεωρητικά) έχει μεγάλη πιθανότητα να ανοιχτεί.

Όλες αυτές οι τεχνικές μπορούν να οδηγήσουν σε επιτυχημένες διαδικτυακές επιθέσεις, η χρησιμοποίηση κακόβουλων συνδέσμων ή λογισκμικων είναι μέρος των επιθέσεων. Συνεπώς, είναι κρίσιμο για τους ανθρώπους να αναγνωρίζουν αυτές τις αρχές και στρατηγικές ώστε να προστατέψουν τους εαυτούς τους, αυτό είναι όμως αρκετά δύσκολο αφού βασιζεται στην ουσία της ανθρώπινης οντότητας - ο τρόπος με τον οποίο σκεφτόμαστε και συμπεριφερόμαστε.

Funded by the Erasmus+ Programme of the European Union

2.3.Ηλεκτρονικό ψάρεμα κατά τη διάρκεια του COVID-19

Κατά την διάρκεια της κρίσης και των καταστροφών, τείνουμε να βασιζόμαστε στους υπολογιστές, στις κινητές σκυσκευές και προφανώς στο ίντερνετ, για να δουλέψουμε, να επικοινωνήσουμε με άλλους ανθρώπους, να βρουμε, να κοινοποιήσουμε και να λάβουμε πληροφορίες, να ψωνίσουμε, κλπ.

Η πανδημία του COVID-19 υπογράμμισε την αδυναμία μας και παρουσίασε την πιθανή ατυχή επίδραση τους διαδικτυακού εγκλήματος στην καθημερινότητά μας σε όλο τον κόσμο. Αφού η σωματική απαγόρευση κυκλοφορίας έγινε συνήθεια και όλο και περισσότερος κόσμος έμεινε σπίτι του και δούλεψε απο το σπίτι του, το διαδικτυακό έγκλημα έγινε ευρέως διαδεδομένο ακόμα περισσοτερο.

Οι ερυνητές της Barracuda[9] παρατήρησαν αύξηση 667% σε phishing απάτες μέσα σε μόλις ένα μήνα απο όταν άρχισε η πανδημία στις αρχές του 2020.

Υπάρχουν αποδείξεις οτι οι διαδικτυακοί εγκληματίες συνεχίζουν να εκμεταλλεύονται αυτες τις αδυναμίες προς δικό τους όφελος. Οι διαδικτυακοί εγκληματίες προσάρμοσαν τις υφιστάμενες μορφές διαδικτυακού εγκλήματος στα πλαίσια αυτής της πανδημίας, καταχράστηκαν την αβεβαιότητα της κατάστασης και την ανάγκη του κόσμου για αξιόπιστες πληροφορίες. Οι εγκληματίες χρησιμοποιούσαν την κρίση του COVID-19 ώστε να διεξάγουν κοινωνικά μηχανικές επιθέσεις, ειδικότερα phishing emails μέσω εκτρατειών spam και πιο στοχοπιημένες προσπάθειες όπως επιχειρηματικά email συμβιβασμού[10]:

- Εκτρατείες phishing και διανομή κακόβουλου λογισμικού μέσω φαινομενικά αυθεντικών ιστοσελίδων ή αρχείων που προσφέρουν πληροφορίες ή συμβουλές για τον COVID-19 συνήθιζαν να μολύνει τους υπολογιστές και να εξάγει προσωπικά στοιχεία του χρήστη
- Παραβάτες αποκτούν πρόσβαση στα συστήματα των εταιρειών με το να στοχοποιούν υπαλλήλους οι οποίοι έιναι σε τηλεδιάσκεψε.

Σύμφωνα με την Ευρωπολ, ο αριθμός των διαδικτυακών επιθέσεων είναι σημαντικός και προβλέπεται οτι θα αυξηθεί κι άλλο. Οι διαδικτυακοί εγκληματίες θα συνεχίσουν να καινοτομούν πάνω στην ανάπτυξη διάφορων κακόβουλων λογισμικών και λυτρισμικών θεματικών πακέτων γύρω απο την πανδημία του COVID-19 και των εμβολίων γενικότερα.

[9] Barracuda Networks is the worldwide leader in Security, Application Delivery and Data Protection Solutions
[10] Council of Europe (2020): Cybercrime and Covid, URL: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (accessed 12.02.2021)

Οι διαδικτυακοί εγκληματίες πιθανόν να επιδιώξουν να εκμεταλλευτούν τον αυξανόμενο ρυθμό των τεχνικών επίθεσης αφού ένας μεγαλύτερος αριθμός εργαζομένων έχουν υιοθετήσει και συνεχίζουν να υιοθετούν την απομακρισμένη εργασία και επιτρέπουν τις συνδέσεις στα συστήματα των οργανισμών[11].

[11] EUROPOL (2020): Pandemic profiteering - how criminals exploit the COVID-19 crisis

3. ΈΡΕΥΝΑ ΓΙΑ ΜΑΘΗΤΕΣ, ΥΠΑΛΛΗΛΟΥΣ ΚΑΙ ΔΙΕΥΘΥΝ ΣΥΜΒΟΥΛΟΥΣ

3.1. Η μεθοδολογία της συλλογής δεδομένων

Ως μέρος του πεδίου της εργασίας, οι εταίροι της κοινοπραξίας του έργου CyberPhish ετοίμασαν και ξεκίνησαν μια έρευνα, απευθυνόμενη σε φοιτητές, εκπροσώπους επιχειρήσεων και διευθύνοντες συμβούλους από τη Λιθουανία, τη Λετονία, την Εσθονία, τη Μάλτα και την Κύπρο. Οι συνεργάτες είχαν ως στόχο να πάρουν μέρος τουλάχιστον 70 συμμετέχοντες (συμπεριλαμβανομένων 20 εκπροσώπων επιχειρήσεων και 10 διευθύνων σύμβουλος) στην έρευνα σε κάθε χώρα εταίρο.

Με βάση την έρευνα που διεξήχθη και την ανατροφοδότηση απο τα σχόλια όλων των συνεργατών, ετοιμάστηκε η αγγλική έκδοση της έρευνας, η οποία αργότερα μεταφράστηκε και διαμορφώθηκε διαδικτυακά στα αγγλικά, τα λιθουανικά και τα λετονικά. Η έρευνα ξεκίνησε στα μέσα Δεκεμβρίου 2020 και ολοκληρώθηκε στα τέλη Ιανουαρίου 2021.

Οι κύριοι στόχοι της έρευνας ήταν:

- Η αναγνώριση της επίγνωσης των ανθρώπων στον τομέα του ηλεκτρονικού ψαρέματος και διαφορετικά είδη ηλεκτρονικού ψαρέματος
- Η αγαγνώριση του πώς οι άνθρωποι καταλαβαίνουν τις επιθέσεις ηλεκτρονικού ψαρέματος
- Η αναγνώριση του χάσματος στον τομέα των δεξιοτήτων

Η έρευνα συνδύασε ερωτήσεις που σχετίζονται με την γνώση της ψυχολογίας και της πληροφοτικής, την προσέγγιση στην κριτική σκέψη, καθώς και παραδείγματα ηλεκτρονικού ψαρέματος για τους ερωτηθέντες για να αξιολογήσουν τις γνώσεις τους «στην πράξη». Κάθε παράδειγμα ηλεκτρονικού ψαρέματος βασίστηκε σε 6 αρχές πειθούς που ανέπτυξε ο Δρ Robert B. Cialdini. Συνολικά, η έρευνα χωρίστηκε σε διάφορα μέρη και συγκέντρωσε δεδομένα σχετικά με:

- Προσωπικές πληροφορίες - συμπεριλαμβανομένου του φύλου, του επιπέδου εκπαίδευσης και της κατάστασης απασχόλησης ·
- Γενικές γνώσεις και συμπεριφορές στον τομέα του ηλεκτρονικού ψαρέματος.
- Προσωπική εμπειρία στον τομέα του ηλεκτρονικού ψαρέματος.
- Αναγνωρίζοντας επιθέσεις ηλεκτρονικού ψαρέματος - υποδεικνύοντας κύριες κόκκινες σημαίες.

Funded by the Erasmus+ Programme of the European Union

- Πρακτικά παραδείγματα ηλεκτρονικού ψαρέματος
- Αυτο-αξιολόγηση των δεξιοτήτων κριτικής σκέψης.
- Αποφυγή επιθέσεων ηλεκτρονικού ψαρέματος - γιατί οι επιθέσεις ηλεκτρονικού ψαρέματος είναι επιτυχείς, κοινωνική μηχανική (ανθρώπινα συναισθήματα που εκμεταλλεύονται οι εισβολείς), ενέργειες που πρέπει να ληφθούν.
- Αυτοαξιολόγηση της αυτοπεποίθησης κατά την διάρκεια χρήσης δεξιοτήτων που απαιτούνται για την αποτροπή επιθέσεων ηλεκτρονικού ψαρέματος.

Τα συγκεντρωμένα αυτά δεδομένα θα χρησιμοποιηθούν για τον εντοπισμό των κενών στις δεξιότητες και την προετοιμασία προτάσεων/συμβουλών για ένα νέο πρόγραμμα σπουδών για την ενίσχυση των δεξιοτήτων, της εκπαίδευσης και της ευαισθητοποίησης των χρηστών του διαδικτύου σχετικά με τα τελευταία αναδυόμενα ζητήματα και τις απειλές στον τομέα της ηλεκτρονικής ασφάλειας, ιδίως - το ηλεκτρονικό ψάρεμα.

Συνολικά, με βάση τα αποτελέσματα αυτής της έρευνας καθώς και τη μελέτη που έγινε σχετικά με το υπάρχον πρόγραμμα σπουδών ηελκτρονικής ασφάλειας, η κοινότητα των συνεργατών θα αναπτύξει εκπαιδευτικό υλικό, αυτοαξιολόγηση γνώσεων και δοκιμές αξιολόγησης γνώσεων, καθώς και σενάρια προσομοιώσεων για προπονήσεις.

3.2.Συλλογή Αποτελεσμάτων

Τα αποτελέσματα της έρευνας μεταφέρθηκαν στον Εθνικό Πίνακα Ευρημάτων (που κατασκευάστηκε αναχώρα - Λιθουανία, Λετονία, Εσθονία, Μάλτα και Κύπρος). Σε αυτόν τον πίνακα, οι συνεργάτες συμπεριέλαβαν τα πιο σχετικά αποτελέσματα που συλλέχθηκαν, παρέχοντας πληροφορίες σχετικά με:

- Τον χαρακτηρισμό των ομάδων που συμμετέχουν στην έρευνα.
- Την ανάλυση των αποτελεσμάτων της έρευνας, χρησιμοποιώντας γραφικά και κείμενο.
- Τα βασικά συμπεράσματα και συστάσεων που έγιναν απο τους ερωτηθέντες..
- Τα συμπεράσματα και τις προτάσεις που έγιναν απο τους συνεργάτες για την υποστήριξη των ίδιων στον καθορισμό και την ανάπτυξη άλλων επιτεύξιμων στόχων.

Οι πίνακες παρέχουν μία περίληψη της γνώσης και της συμπρεριφοράς των ερτηθέντων στο θέμα της ηλεκτρονικής ασφάλειας, και πιο συγκεκριμένα του ηλεκτρονικού ψαρέματος. Τα αποτελέσματα αυτών των πινάκων επιτρέπουν στην οργάνωση να

Funded by the Erasmus+ Programme of the European Union

προχωρήσει σε μία σύγκριση μεταύ των χωρών, αναγνωρίζοντας το χάσμα δεξιοτήτων και τις ανάγκες της κάθε χώρας.

3.3.Αποτελέσματα και ανάλυση των ερευνών

3.3.1. Επισκόπηση των ερωτηθέντων

Παρά την μικρή χρονική περίοδο που διεξήχθησαν οι έρευνες, όλες οι χώρες έφτασαν στον ελάχιστο αριθμό των 70 ερωτηθέντων και τα αποτελέσματα της έρευνας συνολικά που συγκεντρώθηκαν ήταν 514 απαντήσεις από την Λιθουανία, την Λετονία, την Εσθονία, την Μάλτα και την Κύπρο.

	Λιθουανία	**Λετονία**	**Εσθονία**	**Μάλτα**	**Κύπρος**
Ερωτηθέντες ανά χώρα	93	76	165	104	76

Table 1. Αριθμός ερωτηθέντων ανα χώρα.

Απο τους 514 ερωτηθέντες - 259 ήταν γυναίκες, 248 ήταν άντρες και 7 ερωτηθέντες προτίμησαν να μην αποκαλύχουν το φύλο τους. Σε όλες τις χώρες, εκτός απο την Εσθονία, ο αριθμός των θηλυκών ερωτηθέντων ήταν μεγαλύτερος απο οτι των αρσενικών ερωτηθέντων.

	Λιθουανία	**Λετονία**	**Εσθονία**	**Μάλτα**	**Κύπρος**
Γυναίκες	63,4%	57,9 %	34,6%	54,8%	55,3%
Άντρες	36,6%	40,8%	63%	45,2%	42,1%
Προτιμούν να μήν πούν	-	1,3 %	2,4%	-	2,6%

Table 2. Ερωτηθέντες ανα γένος

Η πλειοψηφία των ερωτηθέντων ήταν μαθητές (304), ακολούθησαν οι υπάλληλοι (139), ιδιοκτήτες επιχειρήσεων (53), άνεργοι (10) και αυτοαπασχολούμενοι (8).

Funded by the Erasmus+ Programme of the European Union

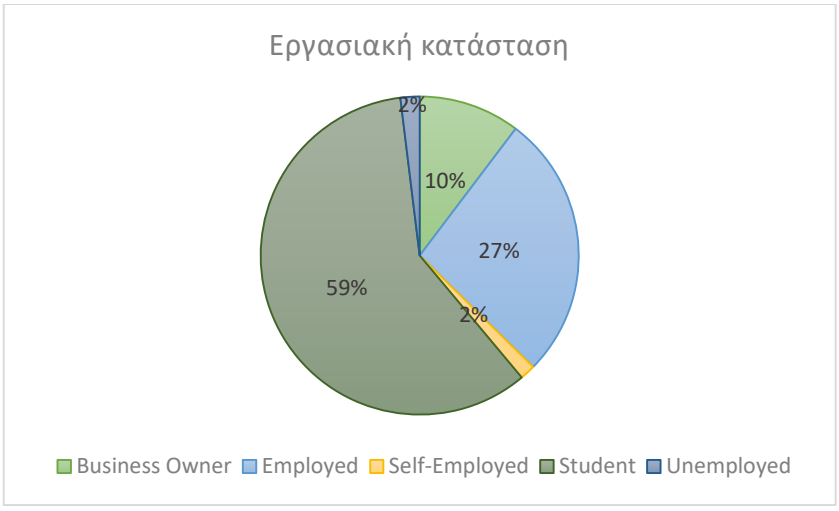


Figure 1. Έρευνα της κατάστασης απασχόλησης των ερωτηθέντων

Οι περισσότεροι ερωτηθέντες της έρευνας είναι μορφωμένοι - με την πλειοψηφία αυτών (38%) να έχουν πτυχίο πανεπιστημίου, ακολουθούν αυτοί με μεταπτυχιακό (23%) και τέλος αυτοί με διδακτορικό (6%)

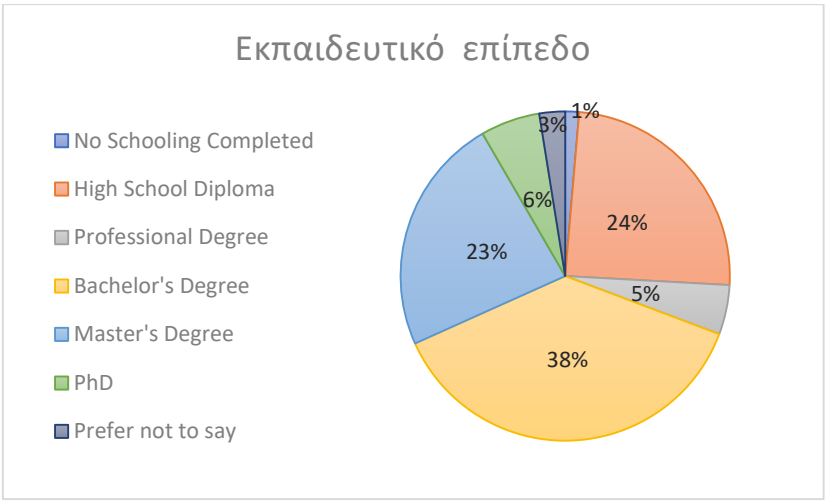


Figure 2. Έρευνα του επιπέδου εκπαίδευσης των ερωτηθέντων

3.3.2. Γενικές γνώσεις και συμπεριφορές

Αν και η πλειοψηφία των ερωτηθέντων (74%) έχουν δηλώσει ότι δεν έχουν συμμετάσχει ποτέ σε καμία επίσημη εκπαίδευση / εργαστήριο / μελέτες σχετικά με την ηλεκτρονική ασφάλεια ή το ηλεκτρονικό ψάρεμα (phishing), περισσότεροι από τους μισούς ερωτηθέντες (56%) έχουν κάνει κάποιου είδους έρευνας πάνω στο θέμα. Αυτό μπορεί να υποδηλώνει ότι τα θέματα ηλεκτρονικής ασφάλειας και ηλεκτρονικού ψαρέματος είναι συναφή σε όλες τις χώρες που

Funded by the Erasmus+ Programme of the European Union

συμμετείχαν στην έρευνα και ενώ οι ερωτηθέντες ενδέχεται να μην έχουν απαραίτητα την ευκαιρία να μελετήσουν το θέμα αυτό σε επίσημο περιβάλλον, είναι πρόθυμοι να αφιερώσουν χρόνο στην έρευνα για να βελτιώσουν τις γνώσεις και τις δεξιότητές τους.

Το 61% των ερωτηθέντων απάντησαν ότι έχουν γνώση του ηλεκτρονικού ψαρέματος (phishing), το 27% δεν είναι σίγουρο και το 12% δεν γνωρίζουν τι είναι το ηλεκτρονικό ψάρεμα (phishing). Όταν τους ζητήθηκε να επιλέξουν τον σωστό ορισμό ηλεκτρονικού ψαρέματος, το 72% των ερωτηθέντων επέλεξε σωστά. Είναι ενδιαφέρον ότι, ενώ στη Μάλτα ο ίδιος αριθμός και στην Εσθονία σχεδόν ο ίδιος αριθμός ερωτηθέντων που ισχυρίστηκαν ότι γνωρίζουν τι είναι το ηλεκτρονικό "ψάρεμα" επέλεξαν τον σωστό ορισμό, στη Λιθουανία, την Κύπρο και τη Λετονία περισσότεροι άνθρωποι επέλεξαν τη σωστή απάντηση από εκείνους που δήλωσαν ότι γνωρίζουν τι είνα το ηλεκτρονικό ψάρεμα. Αυτό μπορεί να υποδηλώνει ότι περισσότεροι ερωτηθέντες από αυτές τις χώρες γνωρίζουν το ηλεκτρονικό ψάρεμα (phishing), αλλά δεν είναι πολύ σίγουροι για τις γνώσεις τους.

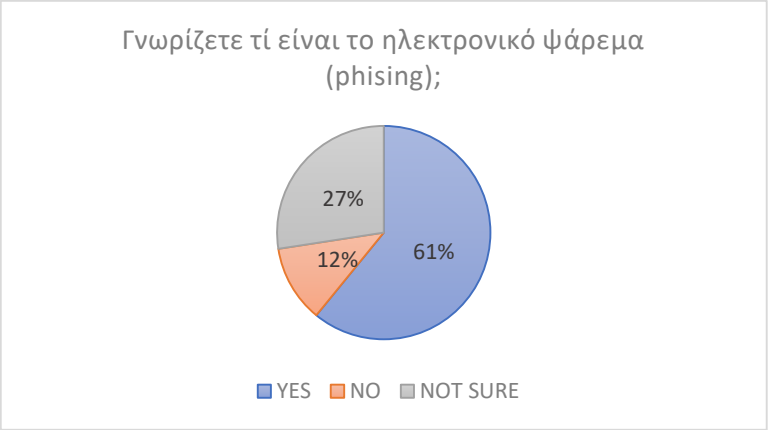


Figure 3. Έρευνα της επίγνωσης των ερωτηθέντων σχετικά με το ηλεκτρονικό ψάρεμα

Σε γενικές γραμμές, σχεδόν οι μισοί από τους ερωτηθέντες (46%) δήλωσαν ότι συχνά φοβούνται να ανοίξουν το σύνδεσμο ή το συνημμένο αρχείο σε ένα email πιστεύοντας ότι θα μπορούσε να είναι ψεύτικο, ενώ το 13% φοβάται πάντα. Μόνο το 3% των ερωτηθέντων δεν φοβάται ποτέ να ανοίξει συνδέσμους / συνημμένα και το 8% φοβούνται σπάνια.

Σχεδόν το ένα τρίτο των ερωτηθέντων (32%) συχνά φοβούνται οτι θα γίνουν στόχοι επιθέσεων ηλεκτρονικού ψαρέματος και το 19% φοβούνται πάντα. Μόνο το 5% των ερωτηθέντων δήλωσαν ότι δεν φοβούνται ποτέ να γίνουν στόχοι επίθεσης ηλεκτρονικού ψαρέματος, ενώ το 17% φοβάται σπάνια.

Αυτό δείχνει ότι η πλειονότητα των ερωτηθέντων γνωρίζουν την πιθανότητα ηλεκτρονικών επιθέσεων και τα βασικά εργαλεία που χρησιμοποιούν οι χάκερ (κακόβουλοι σύνδεσμοι και συνημμένα). Επιπλέον, παρόλο που το 39% των ερωτηθέντων δήλωσαν ότι δεν γνωρίζουν ή δεν είναι σίγουροι τι είναι το ηλεκτρονικό ψάρεμα (phishing), ακόμα δηλαδη και το ήμισυ των

Funded by the Erasmus+ Programme of the European Union

ερωτηθέντων 51% συχνά ή πάντα φοβάται να γίνει στόχος των επιθέσεων ηλεκτρονικού ψαρέματος. Αυτό μπορεί να σημαίνει ότι ακόμη και εκείνοι οι ερωτηθέντες που έχουν δείξει να γνωρίζουν τι είναι το ηλεκτρονικό ψάρεμα (phishing), δεν έχουν τις απαραίτητες γνώσεις για να προστατευτούν ή να εμπιστευθούν τις δεξιότητές τους.

Όταν ρωτήθηκαν για τους διαφορετικούς τύπους ηλεκτρονικού ψαρέματος που γνωρίζουν, οι ερωτηθέντες απο όλες τις χώρες δήλωσαν ότι γνωρίζουν περισσότερο αυτούς τους τύπους ηλεκτρονικού ψαρέματος: «Spray and pray», «Cat phishing» και «Malvertising». Οι ερωτηθέντες σε όλες τις χώρες που συμμετείχαν στην έρευνα, εκτός από τη Λιθουανία, γνωρίζουν επίσης περισσότερο τον τύπο ηλεκτρονικού ψαρέματος "Advanced fee scam".

Figure 4. Οι τύποι των ηλεκτρονικού "ψαρέματος" που γνωρίζουν περισσότερο οι ερωτηθέντες

Από την άλλη πλευρά, οι ερωτηθέντες γνωρίζουν λιγότερο από αυτούς τους τύπους ηλεκτρονικού ψαρέματος: «Whaling», «Clone phishing» και, εκτός από τους ερωτηθέντες από την Κύπρο, γνωρίζουν και τον τύπο «Smishing» *. Οι ερωτηθέντες από τη Μάλτα, την Κύπρο, τη Λιθουανία και τη Λετονία γνωρίζουν επίσης λιγότερο τους τύπους ηλεκτρονικού ψαρέματος «Content injection», ενώ οι ερωτηθέντες στην Εσθονία δήλωσαν ότι γνωρίζουν ως επί το πλείστον αυτόν τον τύπο ψαρέματος.

Figure 5. Τύποι ηλεκτρονικού ψαρέματος που γνωρίζουν λιγότερο οι ερωτηθέντες

Όταν ρωτήθηκαν οι συμμετέχοντες τι είδους συνέπειες είναι πιο πιθανό ή πιο σίγουρα να συμβούν μετά μία επιτυχή επίθεση ηλεκτρονικού ψαρέματος σε ένα άτομο ή εταιρεία, η πλειονότητα των ερωτηθέντων από όλες τις χώρες που ρωτήθηκαν ονόμασαν αυτές τις συνέπειες ως - «κλοπή ευαίσθητων δεδομένων», «απάτη με πιστωτική κάρτα», «κλοπή πληροφοριών πελάτη», «ζημία στη φήμη ενος ανθρώπου» και, εκτός από τους ερωτηθέντες από τη Μάλτα *, «απώλεια ονομάτων χρήστη και κωδικών πρόσβασης». Οι ερωτηθέντες από

Funded by the Erasmus+ Programme of the European Union

όλες τις χώρες που ρωτήθηκαν, εκτός από την Κύπρο **, τείνουν επίσης να πιστεύουν ότι μετά από μια επιτυχή επίθεση ηλεκτρονικού ψαρέματος τα δεδομένα τους πιθανότατα θα πωληθούν σε τρίτους εγκληματίες.

Figure 6. Συνέπειες που είναι πιθανότερο να επιτευχθούν μετά απο μία ηλεκτρονική επίθεση σύμφωνα με τους ερωτηθέντες

Από την άλλη πλευρά, οι ερωτηθέντες από όλες τις χώρες που ερωτήθηκαν πιστεύουν ότι η «απώλεια πνευματικής ιδιοκτησίας» είναι απίθανο να συμβεί μετά από επιτυχή επίθεση ηλεκτρονικού ψαρέματος. Οι ερωτηθέντες από τη Λιθουανία, τη Μάλτα και την Εσθονία είναι επίσης σκεπτικοί σχετικά με την «κλοπή χρημάτων από λογαριασμούς επιχειρήσεων/πελατών» που συνέβη μετά την επίθεση ηλεκτρονικού ψαρέματος.

Λαμβάνοντας υπόψη τη συμπεριφορά των ανθρ'ωπων, σε όλες τις χώρες εταίρους, οι ερωτηθέντες είναι πιο πιθανό να κλικάρουν στο σύνδεσμο ή στο συνημμένο αρχείο στο email ή στο μήνυμα ή/ και να παρέχουν ευαίσθητες πληροφορίες εάν: "αποστέλλεται από το αφεντικό ή τον συνάδελφό τους", "αποστέλλεται από την εταιρεία που χρησιμοποιούν τις υπηρεσίες της», «αποστέλλεται από την τράπεζα ή οποιοδήποτε κυβερνητικό ίδρυμα». Στην Κύπρο, οι ερωτηθέντες θα το έκαναν μάλλον εάν το email / μήνυμα «τους ζητήσει να διευκρινίσουν λεπτομέρειες όπως τη διεύθυνση παραγγελίας (π.χ. παραγγελία amazon)», ενώ οι απόψεις αναμειγνύονται στη Λετονία και τη Μάλτα, με σχεδόν ίσο αριθμό των ερωτηθέντων που θα ήταν πολύ πιθανό αλά και πολύ απίθανο να το κάνουν αυτό. Δεν υπάρχουν ανάμικτες απόψεις μεταξύ των ερωτηθέντων από την Εσθονία και τη Λιθουανία, όπου η πλειοψηφία αυτών πολύ πιθανόν θα το έκανε.

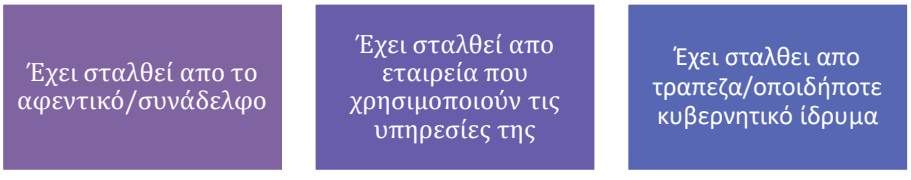


Figure 7. Τύποι email που είναι πιθανότερο οι ερωτηθέντες να κλικάρουν στον σύνδεσμο ή στο συννημένο αρχείο μέσα στο email ή το μήνυμα ή/και να παρέχουν ευαίσθητες πληροφορίες

Funded by the Erasmus+ Programme of the European Union

Τα αποτελέσματα δεν είναι τόσο αναπάντεχα αν ρίξουμε μια ματιά στις 6 αρχές πειθούς που περιγράφηκαν νωρίτερα. Όπως αναφέρθηκε προηγουμένως, οι άνθρωποι τείνουν να ακολουθούν και να εμπιστεύονται περισσότερο την εξουσία ή τους ειδικούς, επομένως πολλοί χάκερ στοχεύουν να πλαστοπροσωπήσουν τόσο κάποιο αξιόπιστο κυβερνητικό ίδρυμα/αρχή όσο και τράπεζες ή CEO. Αυτή η τάση ήταν ορατή και στην έρευνα, όπου το 34% των ερωτηθέντων ισχυρίστηκε ότι πολύ συχνά ή πάντα εμπιστεύονται μηνύματα που φαίνεται να προέρχονται από μια σημαντική οντότητα ή φαίνονται σημαντικά, ενώ το 30% το κάνει μερικές φορές.

Η «Liking principle» παίζει επίσης πολύ σημαντικό ρόλο που σημαίνει ότι οι άνθρωποι είναι πολύ πιο πιθανό να ανταποκριθούν στο αίτημα, ακόμη και αν ακούγονται διαφορετικά από τους συναδέλφους/αφεντικά τους.

Επιπλέον, οι άνθρωποι είναι «πλάσματα της συνήθειας» και τείνουν να τους αρέσει η συνέπεια. Εάν το μήνυμα ηλεκτρονικού ταχυδρομείου αποστέλλεται από την εταιρεία που γνωρίζουν και τις υπηρεσίες που χρησιμοποιούν απο αυτήν, καθώς επίσης και αν πιθανώς έχουν λάβει κάποιο email ή μηνύματα στο παρελθόν, είναι περιττό να πούμε ότι είναι πιο πιθανό να το ανοίξουν και να κλικάρουν σε συνδέσμους/συνημμένα κ.λπ. παρά με κάποια εταιρεία ή υπηρεσίες που δεν χρησιμοποιούν.

Σε όλες τις χώρες εταίρους, οι ερωτηθέντες είναι λιγότερο πιθανό να κάνουν κλικ στο σύνδεσμο ή στο συνημμένο αρχείο μέσα στο email ή στο μήνυμα ή/και να παρέχουν ευαίσθητες πληροφορίες εάν: "τους προσφέρει εμπιστευτικές πληροφορίες (π.χ. πληροφορίες για τους ανταγωνιστές)", "τους ζητά να συμπληρώσουν κάποια έρευνα/δώστε τις επαφές σας μέσω email ή τηλεφώνου για να συμμετάσχετε στο διαγωνισμό και να κερδίσετε ένα βραβείο» ή «αποστέλλεται από την εταιρεία/οργανισμό που γνωρίζουν αλλά δεν χρησιμοποιούν τις υπηρεσίες τους ».

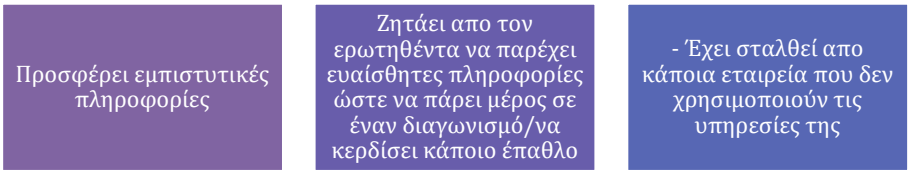


Figure 8. Τύποι μηνυμάτων ηλεκτρονικού ταχυδρομείου που είναι λιγότερο πιθανό να κλικάρουν στο σύνδεσμο ή στο συνημμένο αρχείο στο email ή στο μήνυμα ή/και να παρέχουν ευαίσθητες πληροφορίες οι ερωτηθέντες.

Η πλειονότητα των ερωτηθέντων από την Εσθονία, την Κύπρο και τη Μάλτα, θα ήταν σχεδόν απίθανο επίσης να παρέχει ευαίσθητες πληροφορίες εάν το email ή το μήνυμα «τους ζητά να βοηθήσουν/δωρίσουν σε τοπικές ή διεθνείς φιλανθρωπικές οργανώσεις». Οι ερωτηθέντες από την Κύπρο θα ήταν πιθανόν επίσης να κάνουν κλικ στον σύνδεσμο/συνημμένο και να

παρέχουν ευαίσθητες πληροφορίες εάν «τους προσκαλέσουν σε μια συγκεκριμένη εκδήλωση διαδικτυακά ή εκτός σύνδεσης (π.χ. συνάντηση ζουμ), σε αντίθεση με τους ερωτηθέντες της Λιθουανίας, της Λετονίας, της Εσθονίας και της Μάλτας, οι οποίοι θα ήταν σχετικά απίθανο να το κάνουν αυτό.

3.3.3. Προσωπική εμπειρία με τις επιθέσεις ηλεκτρονικού ψαρέματος

Το 19,8% των ερωτηθέντων ή σχεδόν το ένα πέμπτο αυτών έχουν πέσει θύματα ηλεκτρονικού ψαρέματος στο παρελθόν. Ο πιο συνηθισμένος τρόπος με τον οποίο οι ερωτηθέντες έχουν υποβληθεί σε ηλεκτρονικό ψάρεμα είναι κάνοντας κλικ στο σύνδεσμο στο email ή το μήνυμα, ακολουθώντας είναι η απάντηση στο email ή το μήνυμα και παροχή ευαίσθητων πληροφοριών. Παραδόξως, μόνο οι ερωτηθέντες στην Εσθονία και την Κύπρο έχουν δηλώσει ότι έχουν υποβληθεί σε ηλεκτρονικό ψάρεμα εισάγοντας τα στοιχεία σύνδεσής τους σε ψεύτικο ιστότοπο. Μεταξύ των «άλλων» απαντήσεων οι πιο δημοφιλείς ήταν «συνδυασμός πολλών τεχνικών ηλεκτρονικού ψαρέματος» και «παροχή πληροφοριών σε ψεύτικη έρευνα».

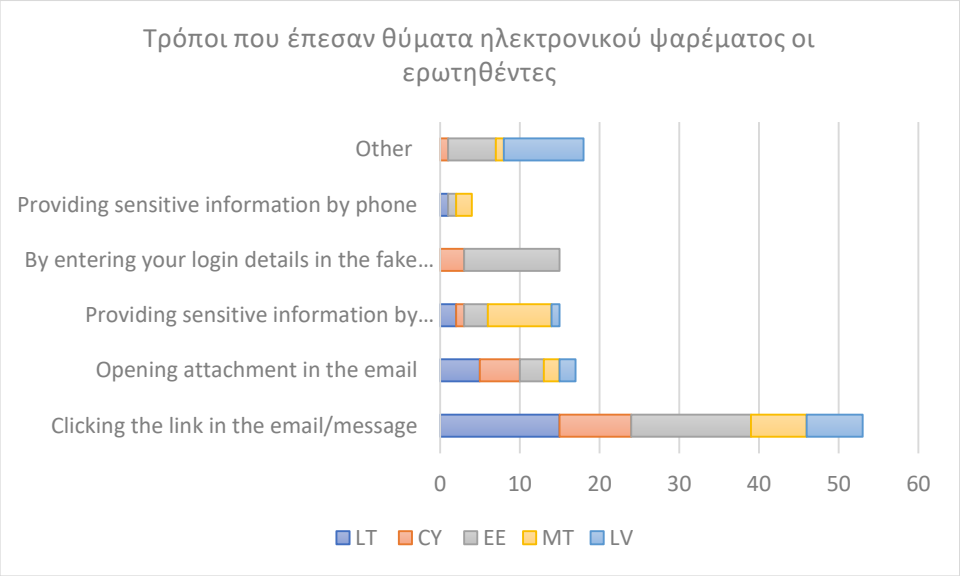


Table 3. Τρόποι που έπεσαν θύματα ηλεκτρονικού ψαρέματος οι ερωτηθέντες στο παρελθόν.

Όταν ζητήθηκε απο τους ερωτηθέντες να υποδείξουν γιατί πιστεύουν οτι έπεσαν θύματα ηλεκτρονικού ψαρέματος, η πλειοψηφία αυτών ισχυρίστηκε ότι ήταν αφηρημένοι, περίεργοι ή βιαζόντουσαν. Μεταξύ και “άλλων” απαντήσεων, η πιο δημοφιλής ήταν οτι οι ερωτηθέντες ήταν νέοι και/ή δεν είχαν επίγνωση του ηλεκτρονικού ψαρέματος.

Funded by the Erasmus+ Programme of the European Union

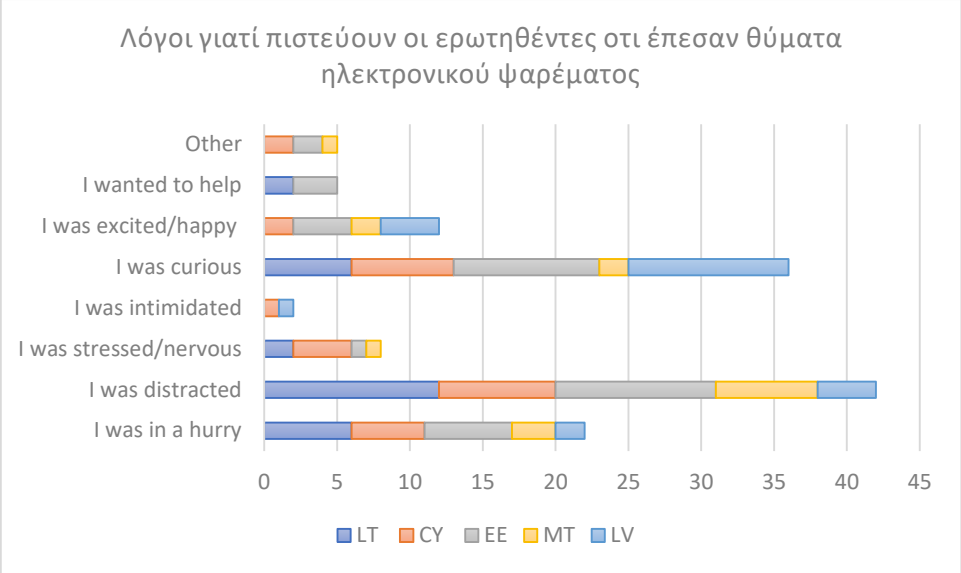


Table 4. Λόγοι γιατί πιστεύουν οι ερωτηθέντες οτι έπεσαν θύματα ηλεκτρονικού ψαρέματος

3.3.4. Αναγνώριση των επιθέσεων ηλεκτρονικού ψαρέματος

Στην έρευνα ζητήθηκε απο τους ενδιαφερόμενους να αξιολογήσουν και να υποδείξουν τα πιο σημαντικά κριτήρια στην αναγνώριση ενός ύποπτου email, γραπτού μηνύματος ή τηλεφωνικής κλήσης, και μηνύματος στα μέσα κοινωνικής δικτύωσης.

Μήνυμα Ηλεκτρονικού Ταχυδρομείου

Όσον αφορά την αναγνώριση των ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου, οι ερωτηθέντες σε όλες τις χώρες είχαν μια ενοποιημένη γνώμη σχετικά με τα πιο σημαντικά κριτήρια που πρέπει να ληφθούν υπόψη. Τα βασικά κριτήρια που αναφέρονται είναι τα εξής: 1) Ο τομέας του αποστολέα (email) δεν φαίνεται γνήσιος (δεν ταιριάζει με τον οργανισμό, περιέχει κρυφό ορθογραφικό λάθος, επιπλέον αριθμούς, γράμματα σε αυτό κ.λπ.). 2) Οι ενσωματωμένοι σύνδεσμοι στο email δεν είναι ίδιοι με τον πραγματικό υπερσύνδεσμο. 3) Ο αποστολέας ζητά απο τον παραλήπτη να επιβεβαιώσει/παρέχει ευαίσθητες πληροφορίες (διαπιστευτήρια σύνδεσης, στοιχεία τράπεζας) μέσω email. 4) Υπάρχουν ορατές ασυνέπειες σε διευθύνσεις email, συνδέσμους και ονόματα τομέα. 5) Το email περιέχει ένα μη αναμενόμενο/ασυνήθιστο συνημμένο αρχείο.

Τα λιγότερο σημαντικά κριτήρια που ανέφεραν οι ερωτηθέντες ήταν 1) Γενικός χαιρετισμός στο email. 2) Δεν υπάρχουν υπογραφές ή στοιχεία επικοινωνίας. 3) Το μήνυμα ηλεκτρονικού ταχυδρομείου δημιουργεί την αίσθηση της περιέργειας, και οτι πρέπει να μάθετε περισσότερα. 4) Το μήνυμα ηλεκτρονικού ταχυδρομείου είναι πολύ καλό για να είναι αληθινό.

Funded by the Erasmus+ Programme of the European Union

Οι ερωτηθέντες από τη Μάλτα επέλεξαν επίσης το στυλ γραφής και ορθογραφίας και λαθών γραμματικής ως λιγότερο σημαντικά.

Γραπτό μήνυμα ή τηλεφωνικη κλήση

Σχεδόν μία ενοποιημένη γνώμη παρατηρήθηκε επίσης μεταξύ των ερωτηθέντων σε όλες τις χώρες που ερευνήθηκαν όσον αφορά τον προσδιορισμό των πιο σημαντικών κριτηρίων για την αναγνώριση ενός ύποπτου γραπτού μηνύματος ή τηλεφωνικής κλήσης. Οι ερωτηθέντες από όλες τις χώρες συμφώνησαν σε αυτές τις πιο σημαντικές «κόκκινες σημαίες» - 1) Ο αποστολέας / καλών ζητά να επαληθεύσει λεπτομέρειες ή να παράσχει ευαίσθητες πληροφορίες ή να στείλει χρήματα. 2) Τηλεφωνικός αριθμός με τον διαφορετικό κωδικό χώρας. και 3) Ο καλών δεν γνωρίζει σωστά τα στοιχεία του εαυτού του (όνομα, θέση, εταιρεία). Οι ερωτηθέντες από όλες τις χώρες που ρωτήθηκαν, εκτός από την Εσθονία, συμφώνησαν επίσης ότι ο ασυνήθιστα μεγάλος τηλεφωνικός αριθμός είναι μία από τις πιο σημαντικές «κόκκινες σημαίες». Επιπλέον, όλοι οι ερωτηθέντες στην έρευνα, εκτός από εκείνους από την Κύπρο, ανέφεραν επίσης ότι το μήνυμα που περιέχει μια προειδοποίηση (π.χ., λογαριασμός που λήγει) και που ασκεί πίεση στον παραλήπτη να λάβει επείγουσα απόφαση είναι επίσης μία από τις σημαντικότερες μεγάλες κόκκινες σημαίες.

Το λιγότερο σημαντικό κριτήριο που υπέδειξαν οι ερωτηθέντες στη Μάλτα, την Εσθονία, τη Λιθουανία και την Κύπρο ήταν ορθογραφικά και γραμματικά λάθη. Αντίθετα, οι Λετονοί ερωτηθέντες επέλεξαν ορθογραφικά και γραμματικά λάθη ως ένα από τα πιο σημαντικά κριτήρια. Οι ερωτηθέντες από σχεδόν όλες τις χώρες που ερωτήθηκαν επίσης απάντησαν ότι δεν είναι τόσο σημαντικό εάν ο καλούντος δεν αναφέρεται σε αυτούς με το όνομα και το επώνυμο τους, εκτός από τους ερωτηθέντες από την Κύπρο, οι οποίοι θεώρησαν ότι θα ήταν ένα από τα πιο σημαντικά κριτήρια για την αναγνώριση μιας ύποπτης κλήσης.

Ένα μήνυμα στα μέσα μαζικής επικοινωνίας

Οι ερωτηθέντες είχαν σχεδόν την ίδια γνώμη όσον αφορά τον εντοπισμό των ύποπτων μηνυμάτων στα κοινωνικά μέσα. Η πλειονότητα των ερωτηθέντων συμφώνησε σε αυτά τα πιο σημαντικά κριτήρια: 1) Το μήνυμα να ζητάει χρήματα. 2) Το μήνυμα να ζητάει λεπτομέρειες επαλήθευσης ή να ζητάει ο παραλήπτης να παρέχει ευαίσθητες πληροφορίες. 3) Το μήνυμα περιέχει έναν αμφίβολο σύνδεσμο και 4) Το προφίλ κοινωνικών μέσων του αποστολέα να φαίνεται ύποπτο (π.χ. νέος λογαριασμός, χωρίς φίλους κ.λπ.). Οι ερωτηθέντες, εκτός από αυτούς από τη Μάλτα, πιστεύουν επίσης ότι το μήνυμα που σας ζητά να εγκαταστήσετε κάποιο πρόγραμμα στον υπολογιστή ή το κινητο σας είναι μία από τις σημαντικότερες κόκκινες σημαίες που υποδηλώνουν ύποπτη δραστηριότητα.

Funded by the Erasmus+ Programme of the European Union

Τα ορθογραφικά και τα γραμματικά λάθη, που δεν είχαν σχέση με τον αποστολέα ή δεν γνωρίζουν τον αποστολέα προσδιορίστηκαν ως τα λιγότερο σημαντικά κριτήρια από τους ερωτηθέντες.

Αναγνώριση Επίθεσης ηλεκτρονικού ψαρέματος	Περισσότερο Σημαντικά Κριτήρια	Λιγότερο Σημαντικά Κριτήρια
Μήνυμα Ηλεκτρονικού Ταχυδρομείου	• Η δικαιοδοσία του αποστολέα (email) δεν φαίνεται γνήσια. • Οι ενσωματωμένοι σύνδεσμοι στο email δεν είναι ίδιοι με τον πραγματικό υπερσύνδεσμο. • Ο αποστολέας ζητά να επιβεβαιώσει/παρέχει ο παραλήπτης ευαίσθητες πληροφορίες. • Υπάρχουν ορατές ασυνέπειες σε διευθύνσεις email, συνδέσμους και ονόματα τομέα. • Υπάρχει ένα απροσδόκητο/ ασυνήθιστο συννημένο αρχείο.	• Γενικός χαιρετισμός; • Χωρίς υπογραφή ή στοιχεία επικοινωνίας. • Το ίδιο το email δημιουργεί περιέργεια, πρέπει να μάθετε περισσότερα.
TEXT MESSAGE OR PHONE CALL Γραπτο μήνυμα ή τηλεφωνική κλήση	• Ο αποστολέας/καλών ζητά οπαραλήπτης να επαληθεύσει λεπτομέρειες ή να παρέχει ευαίσθητες πληροφορίες ή να στείλει χρήματα. • Τηλεφωνικός αριθμός με διαφορετικό κωδικό χώρας. • Ο καλών δεν γνωρίζει σωστά τον εαυτό του (όνομα, θέση, εταιρεία). • Ασυνήθιστος μεγάλος τηλεφωνικός αριθμός[12]. • Το μήνυμα περιέχει μια προειδοποίηση[13]	• Ορθογραφκά και γραμματικά λάθη[14]. • Ο καλών δεν αναφέρεται σε εσάς με το όνομα, επώνυμο σας[15].

[12] Εκτός από τους ερωτηθέντες της Εσθονίας
[13] Εκτός από τους ερωτηθέντες της Κύπρου
[14] Εκτός από τους ερωτηθέντες της Λετονίας
[15] Εκτός από τους ερωτηθέντες της Κύπρου

Funded by the Erasmus+ Programme of the European Union

MESSAGE IN SOCIAL MEADIA Μήνυμα στα μέσα κοινωνικής δικτύωσης	• Το μήνυμα ζητά χρήματα. • Το μήνυμα ζητάει απο τον παραλήπτη λεπτομέρειες επαλήθευσης ή παροχή ευαίσθητων πληροφοριών απο αυτόν. • Το μήνυμα περιέχει έναν αμφίβολο/επικίνδυνο σύνδεσμο. • Το προφίλ στα μέσα κοινωνικής δικτύωσης του αποστολέα φαίνεται ύποπτο (π.χ. νέος λογαριασμός, χωρίς φίλους κ.λπ.). • Το μήνυμα σας ζητά να εγκαταστήσετε κάποιο πρόγραμμα[16].	• Ορθογραφικά και γραμματικά λάθη. • Επικοινωνία του αποστολέα με τον παραλήπτη χωρίς να έχουν επιχειρηματικές σχέσεις μεταξύ τους. • Άγνωστος αποστολέας.

Table 5. Τα περισσότερο και λιγότερο σημαντικά κριτήρια για την αναγνώριση επιθέσεων ηλεκτρονικού ψαρέματος

Σε γενικές γραμμές, όταν πρόκειται για την ένδειξη των βασικών κριτηρίων, οι ερωτηθέντες επικεντρώνονται κυρίως σε «τεχνικά κριτήρια», π.χ. συνδέσμους, τομείς, συνημμένα, κωδικός χώρας κ.λπ. παρά σε ανθρώπινα συναισθήματα (κοινωνική μηχανική) κατά τον εντοπισμό ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου ή μηνυμάτων . Τα ορθογραφικά λάθη ή τα γραμματικά ή ο γενικός χαιρετισμός είναι από τα τελευταία σημεία που πρέπει να αξιολογηθούν από τους ερωτηθέντες.

Ωστόσο, είναι σημαντικό να σημειωθεί ότι ενώ τα «τεχνικά κριτήρια» είναι ένα από τα πρώτα σημεία που πρέπει να παρατηρηθούν και να ελεγχθούν από τους ερωτηθέντες, αυτό δεν σημαίνει ότι δεν λαμβάνουν υπόψη την κοινωνική μηχανική κατά την αξιολόγηση των email και των μηνυμάτων. Όταν τους ρωτήθηκε να προσδιορίσουν τα email/μηνύματα ηλεκτρονικού "ψαρέματος" και τις κύριες "κόκκινες σημαίες" στην έρευνα, η πλειονότητα των ερωτηθέντων από όλες τις χώρες που συμμετείχαν στην έρευνα, επέλεξαν τόσο τα "τεχνικά κριτήρια" όσο και τα κριτήρια που εστιάζονται στα ανθρώπινα συναισθήματα (κοινωνική μηχανική).

[16] Εκτός από τους ερωτηθέντες της Μάλτας

Funded by the Erasmus+ Programme of the European Union

3.3.5. Δεξιότητες κριτικής σκέψης

Η πλειοψηφία των ερωτηθέντων είναι αρκετά θετική για τις δεξιότητες κριτικής σκέψης. Περισσότεροι από τους μισούς ερωτηθέντες (57%) δήλωσαν ότι πολύ συχνά ή σχεδόν πάντα έχουν επαρκή εστίαση και προσοχή στη λεπτομέρεια κατά το άνοιγμα ενός email ή μηνύματος, ενώ το 12% δήλωσε ότι δεν έχουν ποτέ ή έχουν σπάνια επαρκή εστίαση.

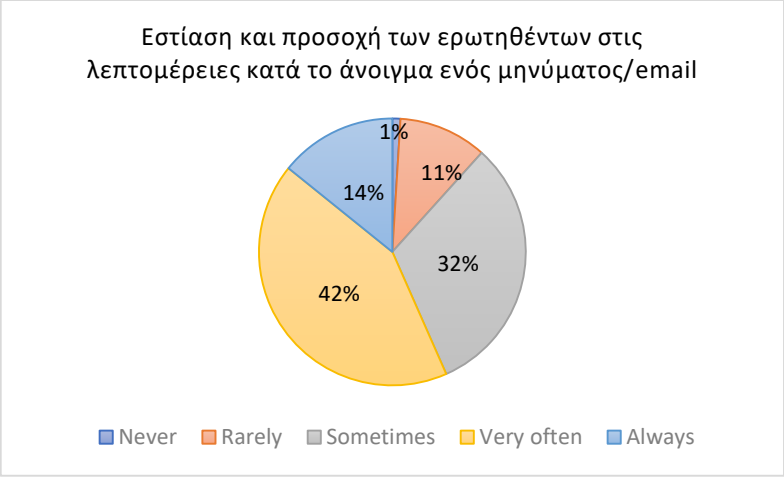


Figure 9. Εστίαση και προσοχή των ερωτηθέντων στις λεπτομέρειες κατά το άνοιγμα ενός μηνύματος/email

Το 71% των ερωτηθέντων ισχυρίζεται ότι πολύ συχνά ή πάντα είναι προσεκτικοί όταν κάνουν κλικ στο σύνδεσμο ή στο συνημμένο αρχείο, ενώ το 11% ισχυρίστηκε ότι ποτέ ή σπάνια έχουν επίγνωση όταν το κάνουν.

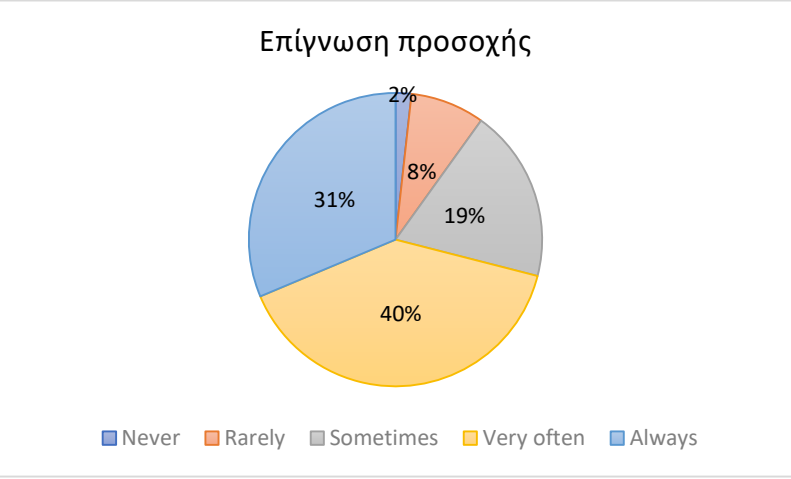


Figure 10. Τα επίπεδα προσοχής των ερωτηθέντων όταν κάνουν κλικ σε έναν σύνδεσμο/ συνημμένο αρχείο.

Το 67% των ερωτηθέντων δήλωσαν ότι πολύ συχνά ή πάντα είναι σε θέση να φανταστούν τους πιθανούς υπαινιγμούς/συνέπειες των αποφάσεών τους, βάσει στοιχείων, όταν λαμβάνουν ένα ύποπτο email ή μήνυμα, ενώ μόνο το 5% των ερωτηθέντων δήλωσαν ότι δεν μπορούν ποτέ ή σπάνια να το οπτικοποιήσουν αυτό.

Funded by the Erasmus+ Programme of the European Union

Το 77% των ερωτηθέντων είναι επίσης πολύ συχνά ή πάντα σε θέση να εξάγει συμπεράσματα, βάσει στοιχείων, όταν λαμβάνουν ένα ύποπτο email ή μήνυμα, ενώ μόνο το 3% των ερωτηθέντων δεν μπορεί ποτέ ή σπάνια να το κάνει.

Η διαφορά μεταξύ του ποσοστού των ερωτηθέντων που μπορούν να οπτικοποιήσουν τις συνέπειες και είναι σε θέση να εξάγουν συμπεράσματα, μπορεί να υποδηλώνει ότι ενώ δεν γνωρίζουν όλοι οι ερωτηθέντες τις συνέπειες του ηλεκτρονικού ψαρέματος, είναι ακόμη σε θέση να εξάγουν συμπεράσματα και να αναγνωρίσουν το email/μήνυμα ηλεκτρονικού ψαρέματος.

Ωστόσο, είναι σημαντικό να υπογραμμιστεί ότι παρά τα αρκετά καλά αποτελέσματα, περίπου το ένα τρίτο των ερωτηθέντων,μόνο, είναι ακόμα σε θέση να απεικονίσει τις συνέπειες και να εξάγει συμπεράσματα.

3.3.6. Αποφυγή επιθέσεων ηλεκτρονικού ψαρέματος

Ζητήθηκε επίσης από τους ερωτηθέντες να αναφέρουν τους κύριους λόγους που, κατά τη γνώμη τους, συμβάλλουν στην επιτυχή επίθεση ηλεκτρονικού ψαρέματος. Οι συμμετέχοντες από όλες τις χώρες που ρωτήθηκαν επέλεξαν 5 βασικούς λόγους: 1) Οι άνθρωποι δεν έχουν επίγνωση/δεν γνωρίζουν τέτοιες επιθέσεις και πώς να τις αποτρέψουν. 2) Οι επιτιθέμενοι εκμεταλλεύονται την ανθρώπινη φύση, βασίζονται στην αλληλεπίδραση και παίζουν με τα ανθρώπινα συναισθήματα και τις ανάγκες. 3) Οι επιτιθέμενοι είναι πραγματικά καλοί στην αναπαραγωγή μηνυμάτων και μηνυμάτων ηλεκτρονικού ταχυδρομείου από νόμιμες εταιρείες, καθιστώντας τους πολύ αληθοφανής και πειστικούς. 4) Οι άνθρωποι δεν δίνουν αρκετή προσοχή / είναι αδαείς. 5) Οι εισβολείς γίνονται πιο προχωρημένοι, στοχεύοντας συγκεκριμένα άτομα, ενώ η χρήση μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι ιδιαίτερα εξατομικευμένη και χρησιμοποιούν συγκεκριμένες πληροφορίες[17].

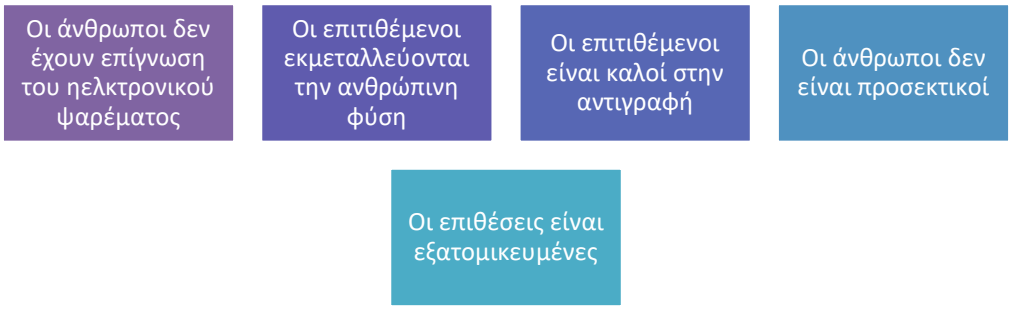


Figure 11. Κύριοι λόγοι που οι επιθέσεις ηλεκτρονικού ψαρέματος είναι επιτυχείς σύμφωνα με τους ερωτηθέντες.

[17] Εκτός από τους ερωτηθέντες της Κύπρου

Funded by the Erasmus+ Programme of the European Union

Οι λιγότερο επιλέξιμοι λόγοι από τους ερωτηθέντες ήταν: 1) Οι άνθρωποι χρησιμοποιούν ξεπερασμένο λογισμικό. 2) Τα εργαλεία ηλεκτρονικού ψαρέματος είναι χαμηλού κόστους και διαδεδομένα. και 3) Το ίδιο το κακόβουλο λογισμικό γίνεται πιο εξελιγμένο[18].

Οι ερωτηθέντες συμφώνησαν ότι οι χάκερ εκμεταλλεύονται συνήθως τα ανθρώπινα συναισθήματα, τις ανάγκες και τις επιθυμίες, ειδικά μέσω της ενίσχυσης του κινήτρου τους προσφέροντας «δώρα» ή δωρεάν κουπόνια, αυξάνοντας την περιέργειά τους και προκαλώντας ανησυχία / άγχος.

Η πλειοψηφία των ερωτηθέντων πιστεύει ότι για να αποφευχθούν οι επιθέσεις ηλεκτρονικού ψαρέματος (phishing) είναι σημαντικό να προσεγγίσουμε αυτό το θέμα από διαφορετικές οπτικές γωνίες: 1) τεχνικός παράγοντας - χρησιμοποιώντας web filter για αποκλεισμό κακόβουλων ιστότοπων, έλεγχος ταυτότητας πολλαπλών παραγόντων/συχνή αλλαγή κωδικών πρόσβασης, καθώς και διπλός έλεγχος όλων των σημαντικών λεπτομερειών (email αποστολέων, συνδέσμων, συνημμένων κ.λπ.) και 2) ανθρώπινος παράγοντας - διατηρώντας ευαίσθητες πληροφορίες για τον εαυτό σας μακριά από τα μέσα κοινωνικής δικτύωσης, προσέχοντας κατά το άνοιγμα των μηνυμάτων ηλεκτρονικού ταχυδρομείου/γραπτών μηνυμάτων/ απαντώντας στο τηλέφωνο και συνεχώς εκπαιδεύοντας τον εαυτό σας σε αυτόν τον τομέα. Η πλειονότητα των ερωτηθέντων στη Λετονία και την Κύπρο πιστεύει επίσης ότι είναι σημαντικό να χρησιμοποιείτε λογισμικό ασφαλείας.

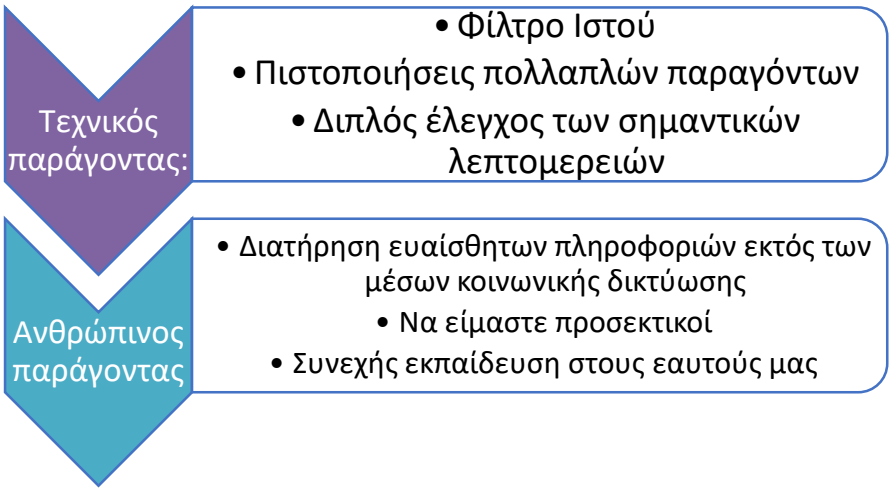


Figure 12. Ενέργειες που πρέπει να ληφθούν για την πρόληψη επιθέσεων ηλεκτρονικού ψαρέματος σύμφωνα με τους ερωτηθέντες

Οι λιγότερο σημαντικές ενέργειες που πρέπει να ληφθούν για την αποφυγή επιθέσεων ηλεκτρονικού ψαρέματος (phishing) σύμφωνα με τους ερωτηθέντες είναι να χρησιμοποιούν ενημερωμένο πρόγραμμα περιήγησης, να συμβαδίζουν με το νεότερο λογισμικό και τα

[18] Εκτός από τους ερωτηθέντες της Μάλτας

Funded by the Erasmus+ Programme of the European Union

εργαλεία που είναι διαθέσιμα ή να χρησιμοποιούν ενημερωμένο λειτουργικό σύστημα, καθώς και τακτική εκπαίδευση στον ηλεκτρονική ασφάλεια/εργαστήρια.

Όταν τους ζητήθηκε να προσδιορίσουν την αυτοπεποίθησή τους στις ικανότητες και τις δεξιότητές τους, οι περιοχές με τους οποίους οι περισσότεροι ερωτηθέντες αισθάνονται πιο άνετοι είναι οι εξής: να μπορούν να βρουν σχετικές και αξιόπιστες πληροφορίες στο διαδίκτυο, να εντοπίζουν επιθέσεις ηλεκτρονικού ψαρέματος και να χρησιμοποιούν το λογισμικό ασφαλείας, τον έλεγχο ταυτότητας πολλαπλών παραγόντων καθώς και φίλτρο ιστού.

Figure 13. Περιοχές στις οποίες οι ερωτηθέντες νιώθουν περισσότερη αυτοπεποίθηση

Λιγότεροι ερωτηθέντες αισθάνονται αυτοπεποίθηση με τις γνώσεις τους σχετικά με την ορολογία της ηλεκτρονικής ασφάλειας/ηλεκτρονικού ψαρέματος (phishing) και τη χρησιμοποίηση αυτών, καθώς και ότι μπορούν να κρυπτογραφήσουν όλες τις ευαίσθητες πληροφορίες της εταιρείας.

Funded by the Erasmus+ Programme of the European Union

4. ΣΥΝΟΨΗ ΚΑΙ ΚΥΡΙΑ ΠΟΡΙΣΜΑΤΑ

Κοινωνικο-δημογραφικά στοιχεία των ερωτηθέντων

- 514 άτομα συμμετείχαν στην έρευνα, εκ των οποίων 259 είναι γυναίκες, 248 άνδρες και 7 άτομα προτιμούν να μην προσδιορίσουν το φύλο τους.

- Η πλειονότητα των ερωτηθέντων είναι μαθητές (304), ακολουθούμενοι από υπαλλήλους (139), ιδιοκτήτες επιχειρήσεων (53), άνεργους (10) και αυτοαπασχολούμενους (8).

- Η πλειονότητα των ερωτηθέντων στην έρευνα είναι υψηλού μορφωτικού επιπέδου - με την πλειονότητα των ερωτηθέντων (38%) να έχουν πτυχίο, ακολουθούμενο από μεταπτυχιακό (23%) και διδακτορικό (6%)

Γενικές γνώσεις και συμπεριφορές

- Παρόλο που το 74% των ερωτηθέντων δεν έχουν συμμετάσχει ποτέ σε κάποια εκπαίδευση/ εργαστήριο ή σε μελέτες στον τομέα της ηλεκτρονικής ασφάλεια σε επίσημο περιβάλλον, περισσότεροι από τους μισούς ερωτηθέντες (54%) έχουν ερευνήσει το ίδιο το θέμα (διάβασαν ένα άρθρο, παρακολούθησαν βίντεο κ.λπ.). Αυτό δείχνει ότι ενώ οι ερωτηθέντες μπορεί να μην έχουν πάντα την ευκαιρία να μελετήσουν ένα θέμα σε επίσημο περιβάλλον, έχουν κίνητρο να βελτιώσουν μόνοι τους τις γνώσεις και τις δεξιότητές τους.

- 61% των ερωτηθέντων ισχυρίστηκαν ότι γνωρίζουν τι είναι το ηλεκτρονικό "ψάρεμα", ενώ το 27% δεν ήταν σίγουρο και το 12% δεν το ήξεραν. Όταν τους ζητήθηκε να επιλέξουν τον σωστό ορισμό του ηλεκτρονικού ψαρέματος, περισσότεροι ερωτηθέντες από τη Λιθουανία, τη Λετονία και την Κύπρο επέλεξαν τη σωστή απάντηση από τον αριθμό των ατόμων που δήλωσαν ότι γνωρίζουν τι είναι το ηλεκτρονικό ψάρεμα. Αυτό μπορεί να υποδηλώνει ότι περισσότεροι ερωτηθέντες από αυτές τις χώρες γνωρίζουν το ηλεκτρονικό ψάρεμα (phishing), ωστόσο ενδέχεται να μην έχουν επαρκή γνώση ή εμπιστοσύνη στις γνώσεις αυτές.

- Το 59% των ερωτηθέντων πολύ συχνά ή πάντα φοβούνται να ανοίξουν το σύνδεσμο ή το συνημμένο πιστεύοντας ότι θα μπορούσε να είναι κακόβουλο, ενώ το 51% πολύ συχνά ή πάντα φοβούνται να γίνουν στόχοι επιθέσεων ηλεκτρονικού ψαρέματος.

Funded by the Erasmus+ Programme of the European Union

Αυτό δείχνει ότι ακόμη και οι ερωτηθέντες που ισχυρίστηκαν ότι γνωρίζουν τι είναι το ηλεκτρονικό "ψάρεμα" φοβούνται ότι θα πέσουν θύματα ηλεκτρονικού ψαρέματος, υποδεικνύοντας ότι δεν υπάρχει επαρκής γνώση ή έλλειψη εμπιστοσύνης στις δεξιότητες τους.

- Οι ερωτηθέντες γνωρίζουν ως επί το πλείστον τους τύπους ψαρέματος “Spray and pray”, “Cat phishing” and “Malvertising”. Αντίθετα, έχουν λιγότερες γνώσεις σχετικά με τις επιθέσεις ηλεκτρονικού ψαρέματος "Whaling", "Clone Phishing" και "Smishing".

- Οι ερωτηθέντες πιστεύουν ότι μετά από επιτυχή επίθεση ηλεκτρονικού ψαρέματος, οι συνέπειες που είναι πιθανότερο να συμβούν είναι - κλοπή ευαίσθητων δεδομένων ή πληροφοριών κάποιου πελάτη, απάτη με πιστωτικές κάρτες και ζημιές στη φήμη ενός προσώπου. Η πλειοψηφία των ερωτηθέντων, εκτός από τη Μάλτα, πιστεύουν επίσης ότι η επιτυχής επίθεση ηλεκτρονικού ψαρέματος μπορεί να οδηγήσει σε απώλεια ονομάτων χρήστη και κωδικών πρόσβασης. Επιπλέον, τα δεδομένα που πωλούνται σε τρίτους εγκληματίες είναι επίσης πιθανότερο να συμβούν όπως απάντησαν ερωτηθέντες από όλες τις χώρες της έρευνας εκτός από την Κύπρο. Αντιθέτως, οι ερωτηθέντες πιστεύουν ότι η απώλεια πνευματικής ιδιοκτησίας είναι λιγότερο πιθανό να συμβεί μετά από επιτυχή επίθεση ηλεκτρονικού ψαρέματος.

- Οι ερωτηθέντες από τη Λιθουανία, τη Μάλτα και την Εσθονία είναι επίσης επιφυλακτικοί σχετικά με την «κλοπή χρημάτων από λογαριασμούς επιχειρήσεων/πελατών» που συνέβη μετά την επίθεση ηλεκτρονικού ψαρέματος.

- Οι ερωτηθέντες είναι πιο πιθανό να κάνουν κλικ στο σύνδεσμο ή στο συνημμένο μήνυμα στο μήνυμα ηλεκτρονικού ταχυδρομείου ή στο μήνυμα εάν αποστέλλονται από το αφεντικό ή κάποιον συνάδελφο, κάποια εταιρεία που χρησιμοποιούν τις υπηρεσίες της ή από κάποια τράπεζα ή κυβερνητικό ίδρυμα που συναναστρέφονται. Φαίνεται ότι οι αρχές του «πειρασμού», της «εξουσίας» και της «συμπάθειας» είναι αυτές που πιθανότατα θα ανταποκρίνονταν στους ερωτηθέντες.

- Οι ερωτηθέντες είναι λιγότερο πιθανό να κάνουν κλικ στο σύνδεσμο ή στο συνημμένο αρχείο στο email ή το γραπτό μήνυμα εάν προσφέρει εμπιστευτικές πληροφορίες, ζητάει απο τους παραλήπτες να παρέχουν ευαίσθητες πληροφορίες για να λάβουν μέρος στο διαγωνισμό για να κερδίσουν ένα έπαθλο ή αποστέλλονται

από καποία εταιρεία, κάποια υπηρεσία που δεν χρησιμοποιούν. Φαίνεται ότι η αρχή της «αμοιβαιότητας» της πειθούς είναι εκείνη στην οποία οι ερωτηθέντες θα ήταν λιγότερο πιθανό να ανταποκριθούν.

Η εμπειρία των ερωτηθέντων στον τομέα του ηλκετρονικού ψαρέματος

- Σχεδόν κάθε 5ος ερωτώμενος έχει πέσει θύμα ηλεκτρονικού ψαρέματος στο παρελθόν. Οι κύριοι τρόποι με τους οποίους οι ερωτηθέντες έπεσαν θύματα ήταν κάνοντας κλικ σε κάποιον σύνδεσμο ή παρέχοντας ευαίσθητες πληροφορίες μέσω email ή μηνύματος. Μόνο οι ερωτηθέντες στην Κύπρο και την Εσθονία ανέφεραν ότι έχουν υποστεί ψαρέματα εισάγοντας τα στοιχεία τους σε κάποιον πλαστό/ψεύτικο ιστότοπο.

- Οι κύριοι λόγοι για τους οποίους έχουν πέσει θύματα ηλεκτρονικού ψαρέματος οι ερωτηθέντες είναι οτι ήταν αποσπασμένοι, περίεργοι ή βιαστικοί. Μερικοί από τους ερωτηθέντες ανέφεραν επίσης ότι δεν γνώριζαν τι είναι το ηλεκτρονικό ψάρεμα.

Αναγνώριση επιθέσεων ηλεκτρονικού ψαρέματος

- Όσον αφορά τα κύρια κριτήρια ή τις «κόκκινες σημαίες» που χρησιμοποιούνται για να υποδείξουν email ηλεκτρονικού ψαρέματος, το μήνυμα κειμένου ή την τηλεφωνική κλήση, καθώς και το μήνυμα κοινωνικής δικτύωσης, οι ερωτηθέντες ήταν γενικά πιο επικεντρωμένοι στα «τεχνικά κριτήρια» όπως ο τομέας του αποστολέα, οι ενσωματωμένοι σύνδεσμοι, συνημμένα αρχεία και ορατές ασυνέπειες μεταξύ αυτών καθώς και ασυνήθιστα μεγάλος τηλεφωνικός αριθμός ή διαφορετικός κωδικός χώρας. Οι ερωτηθέντες ανέφεραν επίσης ότι ο αποστολέας/ καλών που ζητά ευαίσθητες πληροφορίες ή χρήματα είναι μία από τις σημαντικότερες «κόκκινες σημαίες». Τα ορθογραφικά ή γραμματικά λάθη, καθώς και ο γενικός χαιρετισμός στις περισσότερες περιπτώσεις είναι τα τελευταία σημεία που πρέπει να αξιολογηθούν από τους ερωτηθέντες.

- Ωστόσο, ενώ τα «τεχνικά κριτήρια» είναι τα πρώτα που παρατηρούνται και να ελέγχονται από τους ερωτηθέντες, λαμβάνουν επίσης υπόψη τα «ανθρώπινα κριτήρια» (κοινωνική μηχανική) κατά την αξιολόγηση των email και των γραπτών μηνυμάτων. Όταν ρωτήθηκαν να προσδιορίσουν τα email/γραπτά μηνύματα ηλεκτρονικού "ψαρέματος" και τις κύριες "κόκκινες σημαίες" στην έρευνα, η πλειονότητα των ερωτηθέντων από όλες τις χώρες που συμμετείχαν στην έρευνα,

Funded by the Erasmus+ Programme of the European Union

επέλεξαν τόσο τα "τεχνικά κριτήρια" όσο και τα κριτήρια που εστιάζονται στα ανθρώπινα συναισθήματα (κοινωνική μηχανική).

Δεξιότητες κριτικής σκέψης

- Η πλειοψηφία των ερωτηθέντων είναι αρκετά θετική για τις δεξιότητες κριτικής σκέψης. Το 57% των ερωτηθέντων δήλωσε ότι πολύ συχνά ή πάντα έχουν επαρκή συγκέντρωση κατά το άνοιγμα μηνυμάτων ηλεκτρονικού ταχυδρομείου ή γραπτών μηνυμάτων, ενώ το 71% ισχυρίστηκε ότι πολύ συχνά ή πάντα προσέχει όταν κάνει κλικ στο σύνδεσμο ή στο συνημμένο αρχείο.

- Το 67% των ερωτηθέντων δήλωσε ότι είναι πολύ συχνά ή πάντα σε θέση να φανταστεί τις πιθανές συνέπειες στις ενέργειές τους όταν λαμβάνουν ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου ή γραπτά μήνυμα, ενώ το 77% των ερωτηθέντων είναι πολύ συχνά ή πάντα σε θέση να εξάγουν συμπεράσματα. Η διαφορά μεταξύ του ποσοστού των ερωτηθέντων που μπορούν να φανταστουμ τις συνέπειες και είναι σε θέση να εξάγουν συμπεράσματα, μπορεί να υποδηλώνει ότι ενώ δεν γνωρίζουν όλοι οι ερωτηθέντες τις συνέπειες του ηλεκτρονικού ψαρέματος, είναι ακόμη σε θέση να εξάγουν συμπεράσματα και να αναγνωρίσουν το email/ γραπτό μήνυμα ηλεκτρονικού ψαρέματος.

- Ωστόσο, είναι σημαντικό να υπογραμμιστεί ότι παρά τα αρκετά καλά αποτελέσματα, περίπου το ένα τρίτο των ερωτηθέντων,μόνο, είναι ακόμα σε θέση να απεικονίσει τις συνέπειες και να εξάγει συμπεράσματα.

Αποφυγή επιθέσεων ηλεκτρονικού ψαρέματος

- Οι ερωτηθέντες επέλεξαν τους κύριους λόγους που, κατά τη γνώμη τους, οδηγούν σε επιτυχείς επιθέσεις ηλεκτρονικού ψαρέματος (phishing) - οι άνθρωποι δεν γνωρίζουν το ηλεκτρονικό "ψάρεμα" και πώς να το αποτρέψουν, οι επιτιθέμενοι εκμεταλλεύονται την ανθρώπινη φύση και είναι επίσης καλοί στην αναπαραγωγή μηνυμάτων ηλεκτρονικού ταχυδρομείου και μηνυμάτων από νόμιμες εταιρείες ώστε να ξεγελάσουν/εξαπατήσουν τους ανθρώπους και οι άνθρωποι δεν δίνουν αρκετή προσοχή ή είναι ανίδεοι. Λιγότεροι ερωτηθέντες πιστεύουν ότι τα άτομα που χρησιμοποιούν ξεπερασμένο λογισμικό, τα εργαλεία ηλεκτρονικού ψαρέματος είναι χαμηλού κόστους ή διαδεδομένα, καθώς και το κακόβουλο λογισμικό που γίνονται

Funded by the Erasmus+ Programme of the European Union

πιο εξελιγμένα είναι οι κύριοι λόγοι πίσω από τις επιθέσεις ηλεκτρονικού ψαρέματος.

- Οι ερωτηθέντες πιστεύουν ότι οι χάκερ εκμεταλλεύονται ως επί το πλείστον την περιέργεια, την ανησυχία ή το άγχος του ανθρώπου, καθώς και τα κίνητρα χρήσης, όπως «δωρεάν δώρα» ή «κουπόνια».

- Προκειμένου να αποφευχθούν οι επιθέσεις ηλεκτρονικού ψαρέματος, οι ερωτηθέντες πιστεύουν ότι είναι σημαντικό να το προσεγγίσουμε από 2 διαφορετικές οπτικές γωνίες, όπως «τεχνικός παράγοντας» και «ανθρώπινος παράγοντας» χρησιμοποιώντας τα κατάλληλα εργαλεία και στρατηγικές για την κάλυψη και των δύο. Για παράδειγμα, ο "τεχνικός παράγοντας" περιλαμβάνει τη χρήση φίλτρου ιστού, τον έλεγχο ταυτότητας πολλών παραγόντων και τον έλεγχο σημαντικών λεπτομερειών, όπως το email του αποστολέα, συνδέσμους και συνημμένα αρχεία κ.λπ.

- Είναι ενδιαφέρον ότι, ενώ η πλειοψηφία των ερωτηθέντων πιστεύει ότι είναι σημαντικό να εκπαιδεύεται συνεχώς σε αυτόν τον τομέα, λιγότεροι ερωτηθέντες πιστεύουν ότι χρειάζονται τακτικές εκπαιδεύσεις ή εργαστήρια ηλεκτρονικής ασφάλειας. Αυτό, ωστόσο, αντιστοιχεί στα δεδομένα, ότι σχεδόν οι μισοί από τους ερωτηθέντες μελετούν αυτό το θέμα μόνοι τους.

- Σε γενικές γραμμές, οι ερωτηθέντες δίνουν μεγαλύτερη έμφαση στην ικανότητα του ανθρώπου να αξιολογεί και να εντοπίζει επιθέσεις ηλεκτρονικού ψαρέματος (phishing), αντί να βασίζεται στο λειτουργικό σύστημα του υπολογιστή, το λογισμικό και τα διαθέσιμα εργαλεία.

- Όταν τους ζητήθηκε να αξιολογήσουν τις δεξιότητές τους, οι ερωτηθέντες, στην πλειοψηφία των περιοχών που αισθάνονται πιο άνετοι είναι ότι μπορούν να βρουν τις σχετικές και αξιόπιστες πληροφορίες στο διαδίκτυο, να εντοπίσουν επιθέσεις ηλεκτρονικού "ψαρέματος" και να χρησιμοποιήσουν το λογισμικό ασφαλείας, τον έλεγχο ταυτότητας πολλών παραγόντων καθώς και το φίλτρο ιστού.

- Λιγότεροι ερωτηθέντες αισθάνονται αυτοπεποίθηση με τις γνώσεις τους σχετικά με την ορολογία της ηλεκτρονικής ασφάλειας/ηλεκτρονικού ψαρέματος (phishing) και τη χρησιμοποίηση αυτών, καθώς και ότι μπορούν να κρυπτογραφήσουν όλες τις ευαίσθητες πληροφορίες της εταιρείας.

Funded by the Erasmus+ Programme of the European Union

5. ΒΙΒΛΙΟΓΡΑΦΙΑ

1. European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020
2. EUROSTAT (2020): Is internet use safer today?, URL https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb/default/table?lang=en (accessed 11.02.2021)
3. Proofpoint (2019): Human Factor Report 2019, URL https://www.proofpoint.com/us/resources/threat-reports/human-factor (accessed 12.02.2021)
4. European Union Agency for Cybersecurity (2020): Phishing - ENISA threat landscape 2019-2020
5. Deloitte (2019): Understanding Phishing Techniques URL https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf (accessed 112.02.2021)
6. EUROPOL (2020): Internet Organised Crime Threat Assessment 2020
7. NCC group (2020) :Psychology of the Phish: Leveraging the Seven Principles of Influence, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433 (accessed 12.02.2021)
8. Council of Europe (2020): Cybercrime and Covid, URL: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (accessed 12.02.2021)
9. EUROPOL (2020): Pandemic profiteering - how criminals exploit the COVID-19 crisis

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

Παράρτημα 1. Έρευνα "Αξιολόγηση των δεξιοτήτων και ανανγώριση των διαδικτυακων/phishing επιθέσεων"

ΤΜΉΜΑ 1: Προσωπικά Δεδομένα

1. **Όνομα**:.....(προεραιτικό)
2. **Διεύθυνση ηλεκτρονικού ταχυδρομείου:**..... (προεραιτικό - αν θα θέλατε να λάβετε ενημερώσεις όσο ανφορά το πρότζεκτ και να συμμετέχετε στο πρόγραμμα ελέγχου του δοκιμαστικού προγράμματος παρακαώ συμπληρώστε το email σας)

3. **Φύλο**

- Αρσενικό
- Θηλυκό
- Προτιμώ να μην πω

4. **Επίπεδο Εκπαιδευσης**

- Επίπεδο Εκπαιδευσης
- Δεν πραγματοποιήθηκε σχολείο
- Δίπλωμα γυμνασίου/λυκείου
- Επαγγελματικο πτυχίο
- Πτυχίο Πανεπιστημίου
- Μεταπτυχιακό πτυχίο
- Πτυχίο Γιατρού
- Προτιμώ να μην πώ
- Άλλο: .....

5. **Επαγγελματική Κατάσταση**

- Ιδιοκτήτης Επιχείρησης
- Υπάλληλος
- Αυτοαπασχολούμενος
- Μαθητής
- Συνταξιούχος
- Άνεργος
- Άλλο.....

ΤΜΗΜΑ 2: Γενική γνώση & συμπεριφορές

7. **Πόσο πιθανό είναι να πατήσετε/κλικάρετε τον σύνδεσμο ή το αρχείο στο email ή το μήνυμα και/ή να δώσετε ευαίσθητο περιεχόμενο**:

Funded by the Erasmus+ Programme of the European Union

	Πολύ απίθανο	Απίθανο	Ουδέτερο	Πιθανό	Πολύ πιθανό
Προσφορά κουπονιού ή έκπτωσης σε κάποιες αγορές					
Παροχή προσφορών σε αποκλειστικές προσφορές					
Πρόσκληση σε συγκεκριμένο γεγονός/εκδήλωση είτε είσαι είται δεν είσαι συνδεδεμένος στο διαδίκτυο (π.χ. zoom meeting)					
Συμπλήρωση της έρευνας/ παροχή του email ή των επαφών του κινητού σου ώστε να συμμετέχεις σε διαγωνισμό και να κερδίσεις έπαθλο					
Προσφορα εμπιστευτικών πληροφοριών (π.χ. πληροφορίες για τους ανταγωνιστές σου)					
Σου λέει να διευκρινίσεις τα προσωπικά στοιχεία του λογαριασμού σου ώστε να μην κλείσει/απενεργοποιηθεί (π.χ. λογαριασμό τράπεζας, λογαριασμό Netflix, λογαριασμο Facebook, κλπ.)					
Σου ζητάει να διευκρινίσεις τα στοιχεία σου όσο αναφορα την διεύθυνσή σου για κάποιο δέμα/φορτίο που έχεις παραγγήλει (π.χ. παραγγελία απο την Amazon)					
Σε ενημερώνει για τις νεότερες εξελίξεις σχετικά με κοινωνικά ζητήματα και φυσικές καταστροφές (π.χ., ενημερώσεις σχετικά με την κατλασταση του COVID-19)					
Σου ζητάει να βοηθήσεις/να κάνεις δωρά σε τοπικές ή διεθνής φιλανθρωπίες					
Περιέχει πληροφορίες όσο αναφορά τα χόμπι σου					
Έχει σταλεί απο την τράπεζα ή απο κυβερνητικό ίδρυμα					
Έχει σταλει απο το αφεντικό ή κάποιον συνάδελφο σου					
Έχει σταλεί απο την εταιρεία της οποίας χρησιμοποιείς τις υπηρεσίες της					
Έχει σταλεί απο εταιρεία/οργανισμό που ξέρεις					

Funded by the Erasmus+ Programme of the European Union

αλλά δεν χρησιμοποιείς τις υπηρεσίες αυτών					

8. Έχεις ποτέ συμμετάσχει σε οποιαδήποτε επίσημη εκπαίδευση πώ στο θέμα της διαδικτυακής ασφάλειας ή πιο συγκεκριμένα του phishing?

- Ναί
- Οχι

9. . Έχεις κανει ποτέ έρευνα / ή έχεις ποτέ μελετήσεις για την διαδικτυακή ασφάλεια ή το phishing απο μόνος σου ? (να εχεις διαβάσει κάποιο άρθρο, να έχεις δει κάποιο βίντεο, κλπ.)

- Ναί
- Οχι

10. Ξέρεις τι έιναι το Phishing?

- Ναί
- Οχι
- Δεν είμαι σίγουρος

11. Ποιό απο τα παρακάτω παραδείγματα νομίζεις οτι ταιριάζει περισσότερο στον ορισμό του phishing?

- Ένα διαδικτυακό έγκλημα στο οποίο ενας αριθμός ατόμων εχει έρθει σε επικοινωνία μέσω email για να δελεάσει ένα μεμονωμένο άτομο να παρέχει ευαίσθητες πληροφορίες για τους λογαριασμούς του.
- Είναι ένα είδος αθλήματος για εύρίστηση ή διαγωνισμό
- Ανεπιθύμητα και/ή επαναλαμβανόμενα emails απο ένα άτομο ή εταιρεία προσφέροντας προϊόντα ή υπηρεσίες
- Ένα διαδικτυακό έγκλημα στο οποίο ένας αριθμός ατόμων έχει έρθει σε επικοινωνία με κάποιον, μέσω email, τηλεφώνου ή γραπτού μηνύματος για να δελεάσει το άτομο να του παρέχει εύαισθητα στοιχεία/πληροφορίες

12. Έχεις επίγνωση αυτών των τύπων phishing?

1) *Spray and pray* – κακόβουλα email τα οποία στέλνονται σε οποιαδήποτε διεύθυνση ηλεκτρονικού ταχυδρομείου ώστε να κλέψουν ευαίσθητες πληροφορίες
2) *Spear fishing* - κακόβουλα email τα οποία δημιουργούνται και στέλνονται σε συγκεκριμένα άτομα ή οργανισμούς ώστε να κλέψουν ευαίσθητες πληροφορίες
3) *Whaling* - η προσπάθεια να κλέψουν ευαίσθητες πληροφορίες και συνήθως στοχοποιείται το διοικητικό προσωπικό
4) *Vishing* - αναφέρεται στην απάτη του phishing που πραγματοποιείται μέσω του τηλεφώνου
5) *Smishing* - αναφέρεται στο phishing με μηνύματα SMS, αντί για email, που στοχοποιούν ενα άτομο
6) *Angler Phishing* – σχετικά καινούργιου τύπου απατη, η οποία αναφέρεται σε επιθέσεις οι οποίες υπάρχουν στα μέσα κοινωνικής δικτύωσης χρησιμοποιώντας

ψεύτικες ιστοσελίδες, κλωνοποιημένους ιστοτόπους, όπως και tweets για άμεσα μηνύματα.

7) *Clone Phishing* - τύπος phishing οπου ενα έγκυρο email που έχει παραδοθεί παλαιότερα, χρησιμοποιείται ώστε να δημιουργηθεί ενα πανομοιότυπο email με κακόβουλο περιεχόμενο
8) *Malvertising* - αυτού του τύπου phishing χρησιμοποιεί διαδικτυακές διαφημίσεις ή αναδυόμενα παράθυρα που εμφανίζονται ως διαφημίσεις ώστε να αναγκάσει τους ανθρώπους να πατήσουν/κλικάρουν έναν σύνδεσμο ο οποίος φαινεται έγκυρος, αλλά όμως εγκαθιστά κακόβουλο λογισμικό στον υπολογιστη

	Καθόλους επίγνωση	Λίγη επίγνωση	Μέτρια επίγνωση	Πολύ επίγνωση	Τεράστια επίγνωση
Spray and pray					
Advanced fee scam					
Cat phishing					
Spear phishing					
Whaling					
Whishing					
Smishing					
Clone phishing					
Content Injection					
Malvertising					

13. Τι είδους συνέπειες ειναι πιθανότερο να συμβούν μετά απο μία επιτυχημένη επίθεση phishing σε ένα άτομο ή εταιρεία?

	Σίγουρα οχι	Πιθανόν όχι	Πιθανόν	Πολύ πιθανόν	Σίγουρα
Να έχει κλαπεί η ταυτότητα					
Απάτη της πιστωτικής κάρτας					
Να έχουν κλαπεί ευαίσθητα στοιχεία					
Να έχουν χαθεί ονόματα χρήστη και κωδικοί πρόσβασης					
Εγκατάσταση κακόβουλου λογισμικού					
Να έχουν χαθεί τα πνευματικά δικαιώματα					

Funded by the Erasmus+ Programme of the European Union

Να έχουν κλαπεί πληροφορίες ενός πελάτη					
Να έχουν κλαπεί χρήματα απο επιχειρήσεις/δουλειές και να έχουν κλαπεί λογαριασμοί πελατών					
Να υπάρχει πρόσβαση για μελλοντικές διαδικτυακές επιθέσεις					
Να έχουν πωληθεί στοιχεία σε εγκληματικα τρίτα πρόσωπα/μέρη					
Ζημιά στη φήμη					

ΤΜΉΜΑ 3: Προσωπική εμπειρία

14. Έχεις ποτέφοβηθεί να ανοίξεις έναν σύνδεσμο σε ένα email ή μήνυμα, σκεπτόμενος οτι θα μπορούσε να είναι ψεύτικο?

1 – Ποτέ
2 – Σπάνια
3 – Μερικές φορές
4 – Συχνά
5 – Πάντα

15. Είσαι γενικά φοβισμένος/φοβισμένη να γίνεις στόχος μίας επίθεσης phishing'

1 – Ποτέ
2 – Σπάνια
3 – Μερικές φορές
4 – Συχνά
5 – Πάντα

16. Έχεις πέσει ποτέ θύμα μίας phised επίθεσης?

Περιγραφή: Με την έννοια phised εννοούμε, να έχεις πατήσει/κλικάρει τον κακόβουλο σύνδεσμο/αρχείο/ να έχεις δώσει ευαίσθητες πληροφορίες/στοιχεία, κλπ.

- Ναί
- Οχι

ΤΜΗΜΑ 4 - Επίθεση phishing (μόνο για όσους απάντησαν "ναι" στην ερώτηση 15)

Funded by the Erasmus+ Programme of the European Union

17. Με ποίον τρόπο έπεσες θύμα phishing?

- Με το να πατήσεις/κλικάρεις στο email ή μήνυμα
- Με το να απαντήσεις στο email ή μήνυμα και να δώσεις ευαίσθητες πληροφορίες (π.χ. λεπτομέρειες σύνδεσης)
- Με το να ανοίξεις κάποιο συνημμένο αρχείο στο email
- Με το να δώσεις ευαίσθητες πληροφορίες στο τηλέφωνο
- Άλλο.....

18. Γιατί νομίζεις οτι συνέβη αυτό?

- Ήμουν βιαστικός
- Ήμουν αφηρημένος/δεν πρόσεχα
- Ήμουν αγχωμένος/νευρικός
- Ήμουν φοβισμένος
- Ήμουν παράξενος
- Ήμουν ενθουσιασμένος/χαρούμενος (π.χ., νόμιζα οτι κέρδισα κάποιο έπαθλο/δώρο)
- Ήθελα βοήθεια
- Άλλο.....

ΤΜΉΜΑ 5 - Αναγνώριση μίας επίθεσης phishing

19. Η Πόσο σημαντικά είναι αυτά τα κριτήρια για την αναγνλωριση ενός ύποπτου email?

	Οχι σημαντικό	Λίγο σημαντικό	Μέτρια σημαντικό	Σημαντικό	Πολύ σημαντικό
Γενικός χαιρετισμός στο email (π.χ., Αγαπητέ πελάτη)					
Ο αποστολέας σου ζητάει να επιβεβαιώσεις/ παρέχεις ευαίσθητες πληροφορίες (διαπιστευτήρια σύνδεσης) μέσω email ή τηλεφώνου					
Ο τομέας του αποστολέα (email) δεν δείχνει αυθεντικός (δεν ταιριάζει με του οργανισμού, περιέχει ένα κρυμμένο ορθογραφικό λάθος, έξτρα αριθμούς, γράμματα μέσα σε αυτό, κλπ.)					
Οι ενσωματωμένοι σύνδεσμοι μέσα στο email δεν είναι ίδιοι με τους αληθινούς υπαρσυνδέσμους)					
Υπάρχουν ορατές ασυνέπειες στις διεθύνσεις ηλεκτρονικού ταχυδρομείου , τους συνδέσμους & στα αυθεντικά ονόματα					

Funded by the Erasmus+ Programme of the European Union

Το email περιέχει ένα απρόσμενο/ασυνήθιστο συνημμένο αρχείο					
Υπάρχουν ορθογραφικά και γραμμτικά λάθη μέσα στο email					
Ο τρόπος με τον οποίο είναι γραμμένο το email δεν ταιριάζει με το άτομο/ εταιρεία που συνήθως στέλνει τέτοιου είδους emails					
Αυτή δεν είναι υπογραφη ή πληροφορίες επαφής					
Το email προκαλεί την αίσθηση της επίγουσας ανάγκης, απαιτεί άμεση ενέργεια και σε πανικοβάλλει και σε κάνει να νιώθεις αγχωμένος					
Το email σε κανει να έχεις περιέργεθα, χρειάζετραι να ανακαλύψεις περισσότερα για αυτό					
Το email ειναι πολύ καλό για να είναι αληθινό					

20. Πόσο σημαντικά είναι αυτά τα κριτήρια για την αναγνώριση ενός ύποπτου γραπτού μηνύματος/ τηλεφωνικής κλήσης?

	Οχι σημαντικό	Λίγο σημαντικό	Μέτρια σημαντικό	Σημαντικό	Πολύ σημαντικό
Ασυνήθιστα μεγάλος αριθμός					
Αριθμός με διαφορετικό αριθμό χώρας					
Αποστολέας/Καλών σας ζητάει να επιβεβαιώσετε πληροφορίες ή να παρέχετε ευαίσθητες πληροφορίες ή να στειλετε χρήματα					
Ο Καλών δεν συστήνει τον εαυτό του φυσιολογικά (όνομα, θέση, εταιρεία)					
Ο Καλών δεν αναφέρεται σε εσάς με το όνομα ή το επίθετο					
Τα γραπτά μηνύματα περέχουν κάποιον σύνδεσμο					
Δεν είσαι πελάτης της εταιρείας που σου στέλνει					

Funded by the Erasmus+ Programme of the European Union

μήνυμα ή σε παίρνει τηλέφωνο					
Δεν έχεις καμία σχεση ή καμία επιχειρησιακή σχέση με αυτόν που τηλεφωνεί/ στέλνει το μήνυμα					
Το μήνυμα περιέχει ένα άλλο τηλέφωνο που πρέπει να τηλεφωνήσεις					
Ορθογραφικά/Γραμμτικά λάθη					
Το μήνυμα απο μόνο του περιέχει μία προειδοποίηση (π.χ. λήξη λογαριασμού) και πιέζει τον παραλήπτη να πάρει μια επιτακτική απόφαση.					

21. Πόσο σημαντικά είναι αυτά τα κριτήρια για την ανγώριση ενός ύποπτου μηνύματος στα μέσα κοινωνικής δικτύωσης?

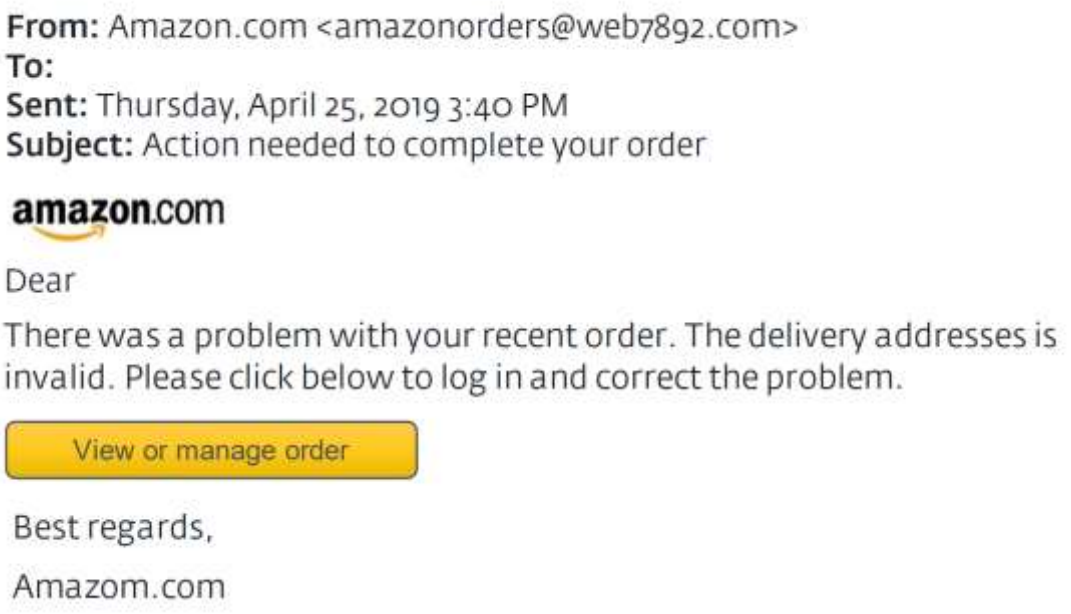
	Καθόλου σημαντικό	Λίγο σημαντικό	Μέτρια σημαντικό	Σημαντικό	Πολύ σημαντικό
Το μήνυμα ζητάει έγκυρες λεπτμέρειες ή την παροχή ευαίσθητων πληροφοριών					
Το μήνυμα ζητάει χρήματα					
Το μήνυμα ζητάει να εγκαταστήσεις κάποιο πρόγραμμα					
Το μήνυμα εμπεριέχει έναν αβέβαιο σύνδεσμο					
Δεν γνωρίζω τον αποστολέα					
Δεν έχω καμία επιχειρησιαή σχέση με τον αποστολέα					
Το προφίλ του αποστολέα στα μέσα κοινωνικής δικτύωσης φαίνεται ύποπτο (π.χ. νέος λογαριασμός, χωρίς φίλους, κλπ.)					
Το μήνυμα περιέχει τίτλο που σου αποσπάει την προσοχή/κινεί το ενδιαφέρον (π.χ. Δεν θα πιστέψεις αυτό το βίντεο!)					
Το στύλ του μηνύματος δεν ταιριάζει με τον αποστολέα (πολύ					

Funded by the Erasmus+ Programme of the European Union

επίσημο/ανεπίσημο κλπ.)					
Ορθογραφικά/Γραμματικά λάθη					

ΤΜΉΜΑ 6 - Παραδείγματα Phishing

Παράδειγμα Phishing 1


From: Amazon.com <amazonorders@web7892.com>
To:
Sent: Thursday, April 25, 2019 3:40 PM
Subject: Action needed to complete your order

amazon.com

Dear

There was a problem with your recent order. The delivery addresses is invalid. Please click below to log in and correct the problem.

View or manage order

Best regards,

Amazom.com

22. Είναι η παραπάνω εικόνα αληθινό email ή phishing email?

- αληθινό
- Phishing Email

ΤΜΉΜΑ 7

Παράδειγμα 1 (μόνο αν απαντήσες "Phishing Email" στην προηγούμενη ερώτηση)

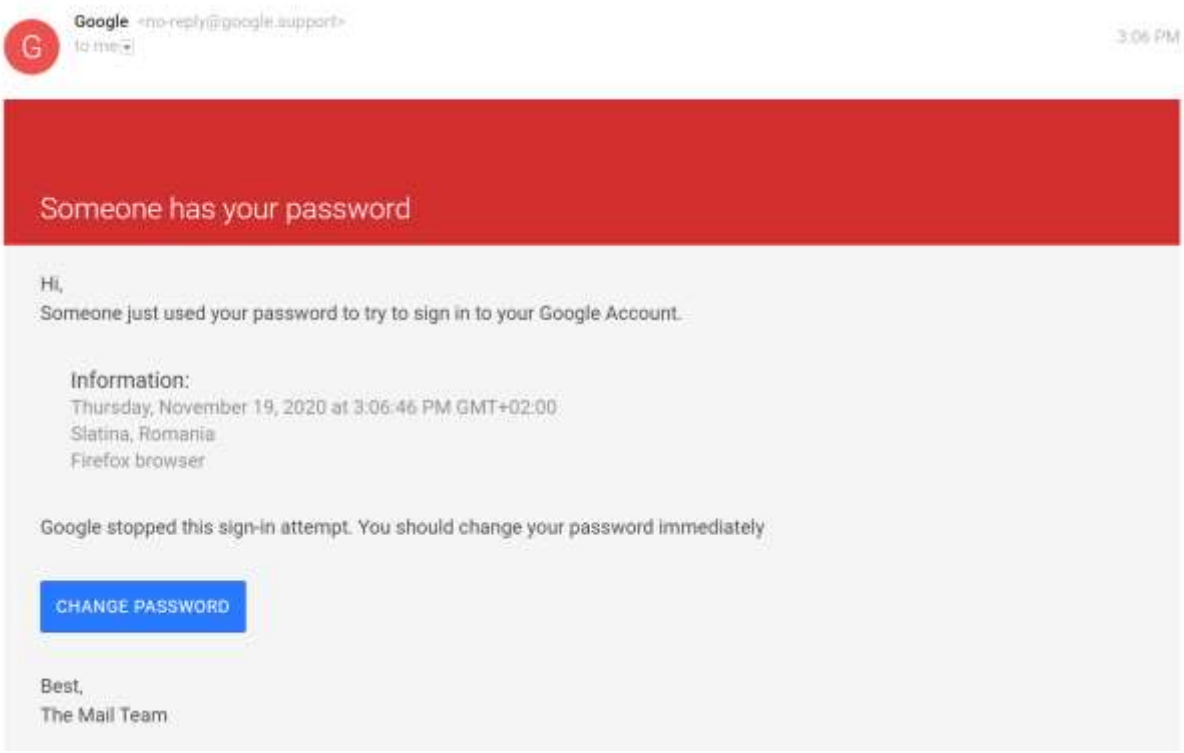
23. Γιατί επέλεξες οτι αυτό το email είναι phishing εμαιλ? Επέλεξε τις "κόκκινες περιοχές ?

- Γενικοί χαιρετισμοί
- Ζητάει για επιβεβαίωση/επικύρωση/λεπτομέρειες ευαίσθητων πληροφοριών
- Ο κλαδος/Το email του αποστολέα
- Ύποπτοι σύνδεσμοι
- Πρόβλημα στις διευθύνσεις ηλεκτρονικού ταχυδρομείου, στους συνδέσμους & στα ονόματα των κλάδων
- Ορθογραφικά και γραμματικά λάθη
- Ύποπτος τρόπος γραφής
- Αίσθηση επείγουσας ανάγκης/ανάγκη για άμεση δράση
- Πολύ καλό για να είναι αληθινό

Funded by the Erasmus+ Programme of the European Union

ΤΜΉΜΑ 8

Παράδειγμα Phishing 2



24. Είναι η παραπάνω εικόνα αληθινό email ή phishing email?

- αληθινό
- Phishing email

ΤΜΉΜΑ 9

Παράδειγμα 2 (μονο αν απάντησες "Phishing Email" στην προηγούμενη ερώτηση)

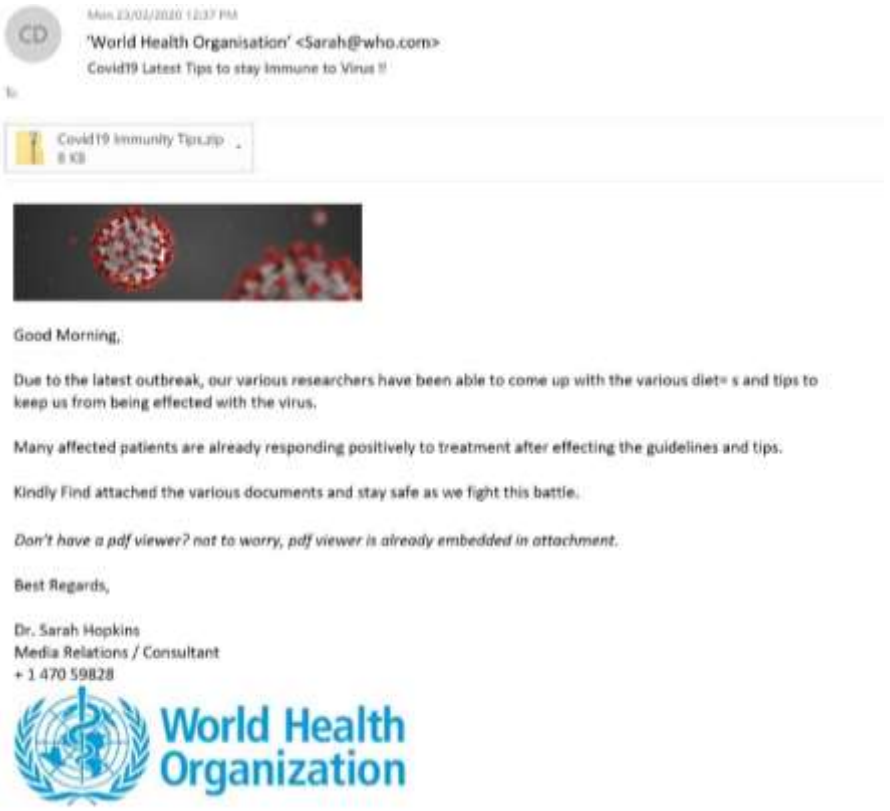
25. Γιατί επέλεξες οτι αυτό το email είναι phishing εμαιλ? Επέλεξε τις "κόκκινες περιοχές"

- Γενικοί χαιρετισμοί
- Ζητάει για επιβεβαίωση/επικύρωση/λεπτομέρειες ευαίσθητων πληροφοριών
- Ο κλαδος/Το email του αποστολέα
- Ύποπτοι σύνδεσμοι
- Πρόβλημα στις διευθύνσεις ηλεκτρονικού ταχυδρομείου, στους συνδέσμους & στα ονόματα των κλάδων
- Ορθογραφικά και γραμματικά λάθη
- Ύποπτος τρόπος γραφής
- Αίσθηση επείγουσας ανάγκης/ανάγκη για άμεση δράση
- Πολύ καλό για να είναι αληθινό

Funded by the Erasmus+ Programme of the European Union

ΤΜΉΜΑ 10

Παράδειγμα Phishing 3



26. Είναι η παραπάνω εικόνα αληθινό email ή phishing email?

- αληθινό
- Phishing email

ΤΜΉΜΑ 11

Παράδειγμα 3 (μονο αν απάντησες "Phishing Email" στην προηγούμενη ερώτηση)

27. Γιατί επέλεξες οτι αυτό το email είναι phishing εμαιλ? Επέλεξε τις "κόκκινες περιοχές"

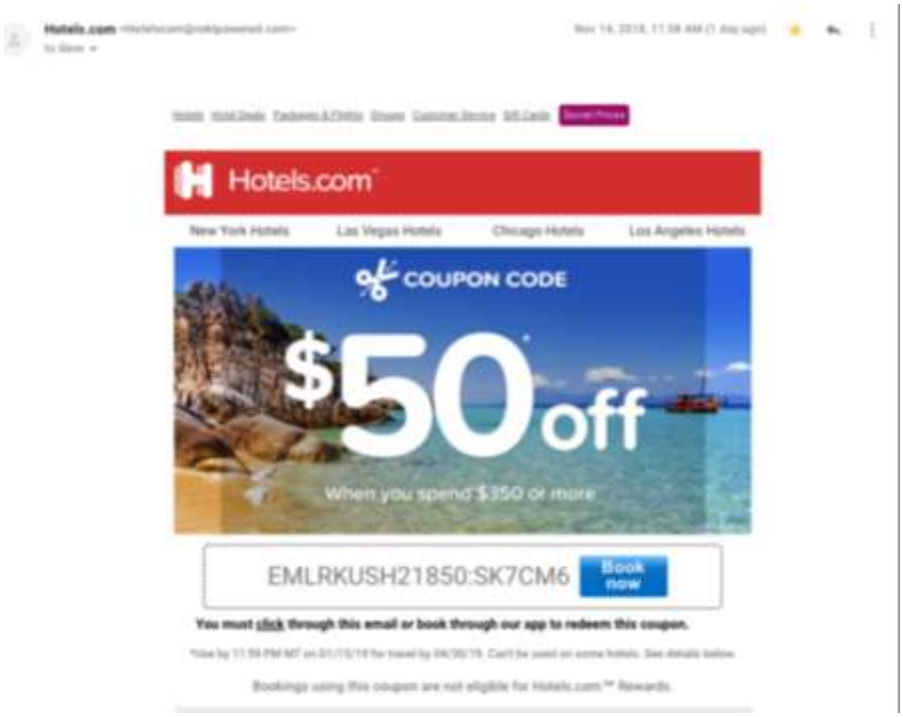
- Γενικοί χαιρετισμοί
- Ζητάει για επιβεβαίωση/επικύρωση/λεπτομέρειες ευαίσθητων πληροφοριών
- Ο κλαδος/Το email του αποστολέα
- Ύποπτοι σύνδεσμοι
- Πρόβλημα στις διευθύνσεις ηλεκτρονικού ταχυδρομείου, στους συνδέσμους & στα ονόματα των κλάδων
- Ορθογραφικά και γραμματικά λάθη

Funded by the Erasmus+ Programme of the European Union

- Ύποπτος τρόπος γραφής
- Αίσθηση επείγουσας ανάγκης/ανάγκη για άμεση δράση
- Πολύ καλό για να είναι αληθινό

ΤΜΉΜΑ 12

Παράδειγμα Phishing 4



28. Είναι η παραπάνω εικόνα αληθινό email ή phishing email?
- αληθινό
- Phishing email

ΤΜΉΜΑ 13

Παράδειγμα 4 (μονο αν απάντησες "Phishing Email" στην προηγούμενη ερώτηση)

29. Γιατί επέλεξες οτι αυτό το email είναι phishing εμαιλ? Επέλεξε τις "κόκκινες περιοχές"
- Γενικοί χαιρετισμοί
- Ζητάει για επιβεβαίωση/επικύρωση/λεπτομέρειες ευαίσθητων πληροφοριών
- Ο κλαδος/Το email του αποστολέα
- Ύποπτοι σύνδεσμοι
- Πρόβλημα στις διευθύνσεις ηλεκτρονικού ταχυδρομείου, στους συνδέσμους & στα ονόματα των κλάδων
- Ορθογραφικά και γραμματικά λάθη
- Ύποπτος τρόπος γραφής
- Αίσθηση επείγουσας ανάγκης/ανάγκη για άμεση δράση

Funded by the Erasmus+ Programme of the European Union

- Πολύ καλό για να είναι αληθινό

ΤΜΉΜΑ 14

Παράδειγμα Phishing 5

From: **Markus** <markusceo@eco1focus.com>
Date: Mon, Dec 7, 2020 at 11:38 AM
Subject: Invoice to be paid
To: Finance department <financedept@ecofocus.org>

Hi Gwen,

Could you do me a favour? Theres pending invoice from one of our providers and because I'm on holiday I need you to take care of it for me bec ause I can't access the accounts from here.
They contacted me and I told them to send through the email to you as well (check spam filter incase it's accidentally blocked!) Just click on the link in their email and transfer the amount to the account they specify.

This needs to be done TODAY so make it high priority.

If you do this for me it would be a huge favour.

Any questions then reply to this email. I can't take calls right now so just stick to replying to this email.

Thanks,
Markus
CEO

30. Είναι η παραπάνω εικόνα αληθινό email ή phishing email?

- αληθινό
- Phishing email

ΤΜΉΜΑ 15

Παράδειγμα 5 (μονο αν απάντησες "Phishing Email" στην προηγούμενη ερώτηση)

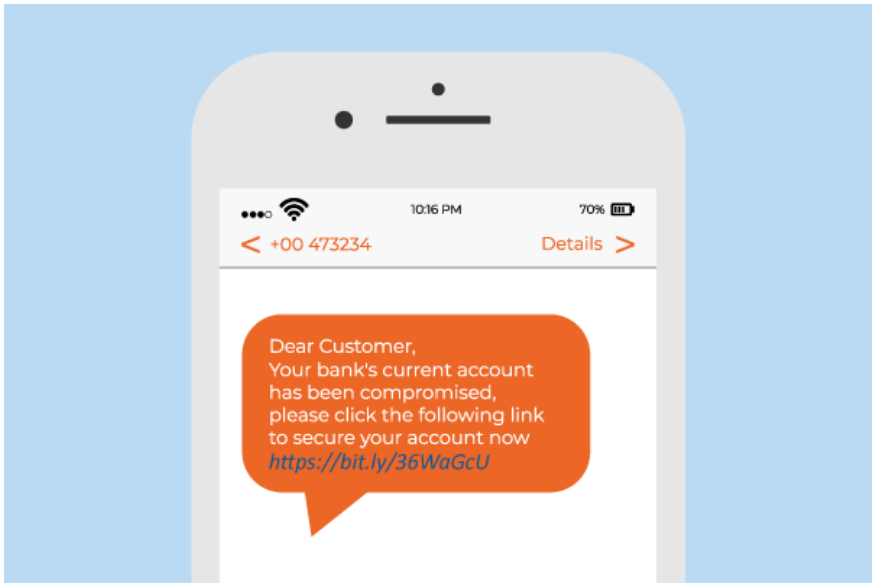
31. Γιατί επέλεξες οτι αυτό το email είναι phishing εμαιλ? Επέλεξε τις "κόκκινες περιοχές"

- Γενικοί χαιρετισμοί
- Ζητάει για επιβεβαίωση/επικύρωση/λεπτομέρειες ευαίσθητων πληροφοριών
- Ο κλαδος/Το email του αποστολέα
- Ύποπτοι σύνδεσμοι
- Πρόβλημα στις διευθύνσεις ηλεκτρονικού ταχυδρομείου, στους συνδέσμους & στα ονόματα των κλάδων
- Ορθογραφικά και γραμματικά λάθη
- Ύποπτος τρόπος γραφής
- Αίσθηση επείγουσας ανάγκης/ανάγκη για άμεση δράση
- Πολύ καλό για να είναι αληθινό

ΤΜΉΜΑ 16

Παάδειγμα Phishing 6

Funded by the Erasmus+ Programme of the European Union



32. Είναι η παραπάνω εικόνα αληθινό email ή phishing email?

- αληθινό
- Phishing text

ΤΜΉΜΑ 17

Παράδειγμα 6 (μονο αν απάντησες "Phishing Email" στην προηγούμενη ερώτηση)

33. Γιατί επέλεξες οτι αυτό το email είναι phishing εμαιλ? Επέλεξε τις "κόκκινες περιοχές"

- Γενικοί χαιρετισμοί
- Ζητάει για επιβεβαίωση/επικύρωση/λεπτομέρειες ευαίσθητων πληροφοριών
- Ο κλαδος/Το email του αποστολέα
- Ύποπτοι σύνδεσμοι
- Πρόβλημα στις διευθύνσεις ηλεκτρονικού ταχυδρομείου, στους συνδέσμους & στα ονόματα των κλάδων
- Ορθογραφικά και γραμματικά λάθη
- Ύποπτος τρόπος γραφής
- Αίσθηση επείγουσας ανάγκης/ανάγκη για άμεση δράση
- Πολύ καλό για να είναι αληθινό

ΤΜΉΜΑ 18 - Αυτοαξιολόγηση: Κριτική σκέψη

33. Χρησιμοποίηση την βαθμίδα απο το 1 μέχρι το 5 για αξιολόγηση:

1 – Ποτέ
2 – Σπάνια
3 – Μερικές φορές
4 – Συχνά
5 – Πάντα

Funded by the Erasmus+ Programme of the European Union

	Ποτέ	Σπάνια	Μερικές φορες	Πολύ συχνά	Πάντα
Εμπιστεύεσαι συνήθως μηνύματα που φαίνεται σαν να εμφανίζονται απο μια σημαντική οργάνωση ή φαίνονται σημαντικά?					
Όταν ανοίγεις ενα email/μήνυμα έχεις επαρκή συγκέντρωση και προσοχή στην λεπτομέρεια?					
Έχεις επίγνωση του τι πατάς/κλικάρεις όταν παραλαμβάνεις ενα email/μήνυμα με σύνδεσμο/ συνημμένο αρχείο?					

34. Όταν λαμβάνεις ένα email που φαίνεται ύποπτο, αξιολογείς:

	Ποτέ	Σπάνια	Μερικές φορες	Πολύ συχνά	Πάντα
Ποιός είναι ο αποστολέας					
Το email του αποστολέα					
Το θέμα του email					
Το στύλ του email (επίσημο, ανεπίσημο, χρήση των λέξεων)					
Φωτογραγίες					
Γραμματικά και ορθογραφικά λάθη					
Σύνδεσμοι/συνημμένα αρχεία					
Υπογραφή και διαπιστευτήρια					

35. Όταν λαμβάνεις ενα ύποπτο email/μήνυμα, είσαι σε θέση να φανταστείς πιθανές συνέπειες/υπονοούμενα της απόφασής σου, βασισμένα σε αποδείξεις?

- Ποτέ
- Σπάνια
- Μερικές φορές
- Πολύ συχνά
- Πάντα

36. Όταν λαμβάνεις ένα email/μήνθμα που φαίνεται ύποπτο, είσαι σε θέση να προβείς σε συμπεράσματα, βασισμενα σε αποδείξεις?

- Ποτέ
- Σπάνια

Funded by the Erasmus+ Programme of the European Union

- Μερικές φορές
- Πολύ συχνά
- Πάντα

ΤΜΉΜΑ 19 - Αποφυγή Επιθέσεων phishing

37. Γιατί οι επιθέσεις phishing είναι επιτυχείς? (Διάλεξε 5 λόγους)

- Οι επιθετιθέμενοι είναι πολύ καλοί στην αντιγραφή μηνυμάτων και email απο αληθινές/κανονικές εταιρείες, που τους κάνει πολύ πειστικούς και αληθοφανείς
- Οι επιτιθέμενοι εκμεταλλεύονται την ανθρώπινη φύση, βασίζονται στην επικοινωνία/αλληλεπίδραση και παίζουν με τα ανθρώπινα συναισθήματα και τις ανθρώπινες ανάγκες
- Οι επιτιθέμενοι έχουν εύκολη πρόσβαση σε προσωπικά δεδομένα και πληροφορίες για ένα συγκεκριμένο άτομο ή εταιρεία στα μέσα κοινωνικής δικτύωσης/ιστοσείδες εταιρείας, στις εφημερίδες, κλπ.
- Οι επιτιθέμενοι γίνονται όλο και και καλύτεροι, στοχοποιούν συγκεκριμένα άτομα καθώς χρησιμοποιούν τα email ειναι αρκετά προωποποιημένοι και χρησιμοποιούν συγκεκριμένες πληροφορίες
- Οι άνθρωποι δεν προσέχουν/είναι αδαής
- Οι άνθρωποι δεν έχουν επίγνωση/δεν γνωρίζουν για τέτοιου είδους επιθέσεις και πώς να τις αποφύγεις
- Οι άνθρωποι χρησιμοποιούν ξεπερασμένο λογισμικό
- Οργανισμοί/Εταιρείες δεν πράττουν αρκετά ώστε να αποτρέψουν αυτές τις επιθέσεις
- Υπάρχει έλλειψη εκπαίδευσης όσο αναφορα το θεμα τις διαδικυακής ασφάλειας και του phishing
- Τα εργαλεία του phishing έχουν χαμηλό κόστος και είναι ευρέως διαδεδομένα
- Το κακόβουλο λογισμικό απο μόνο του γίνεται όλο και πιο προχωρημένο/εκλεπτυσμένο

38. Τι συναισθήματα, ανάγκες και επιθυμίες εκμεταλλεύονται συνήθως οι επιτιθέμενοι?

- Φόβο
- Ανησυχία/’Αγχος
- Πανικό
- Περιέργεια
- Απληστία
- Κίνητρο (Δώρο/Δωρεάν Κουπόνι)
- Επιθυμία για συναισθηματική εκπλήρωση
- Αίσθηση εμπιστοσύνης
- Εξυπξρετικότητα
- Άλλο.....

Funded by the Erasmus+ Programme of the European Union

39. Ποιές πράξεις είναι σημεντικές ώστε να μπορέσει κάποιος να αποφύγει τις επιθέσεις phishing?

	Οχι σημαντικό	Λίγο σημαντικό	Μέτρια σημαντικό	Σημαντικό	Πολύ σημαντικό
Να χρησιμοποιεί ενημερωμένο πρόγραμμα περιήγησης					
Να χρησιμοποιεί ενημερωμένο λειτουργικό σύστημα					
Να συμβασίζεις με τα νεότερα προγράματα & εργαλεία τα οποία είναι διαθέσιμα					
Να χρησιμοποιεί πρόγραμμα ασφαλείας					
Να κρατάει ευαίσθητες πληροφορίες για τον εαυτό του εκτός των έσων κοινωνικής δικτύωσης					
Να χρησιμοποιεί πολυπαραγωντική επαλήθευση/ να αλλάζει κωδικούς συχνότερα					
Να χρησιμοποεί φίλτρο στο πρόγραμμα περιήγησης που χρησιμοποιεί για να μπλοκάρει τις κακόβουλες ιστοσελίδες					
Να έχει μόνιμη εκπαίδευση πανω στο θέμα της διαδικτυκής ασφάλειας					
Να αναπτύξει πολιτική ασφαλείας					
Να κρυπτογραφήσει ολες τις ευαίσθητες πληροφορίες της εταιρείας					
Να είναι προσεκτικός όταν ανοίγει τα email/ μηνύματα/οταν απαντάει στο τηλέφωνο					
Να διπλοτσεκάρει όλες τις σημαντικές λεπτομέρειες (το email του αποστολέα, συνδέσμους, συνημμένα αρχεία, κλπ.)					
Να εμπιστεύεται το ένστικτό του και να χρησιμοποιεί την άποψή του					
Να συνεχίσει να εκπαιδεύει τον εαυτό του πάνω σε αυτο το θέμα					

Funded by the Erasmus+ Programme of the European Union

40. Σε τι βαθμό συμφωνείς με τις δηλωσεις. Έχω αυτοπεποίθηση σε::

	Καθόλου σίγουρος	Λίγο σίγουρος	Μέτρια σίγουρος	Αρκετά σίγουρος	Απόλυτα σίγουρος
Να γνωρίζω τις ορολογίες της διαδικτυακής ασφάλειας και του phishing					
Να βρίσκω τις σχετικές & αξιόπιστές πληροφορίες διαδικτυακά					
Να κάνω σωστές πράξεις/ να παίρνω κατάλληλα μέτρα για να αποτρέψω τις επιθέσεις phishing					
Να αναγνωριζω τις επιθέσεις phishing					
Να διατηρώ τα λογισμικά/προγράμματα ενημερωμένα					
Να χρησιμοποιώ πολυπαραγωντικές επαληθεύσεις					
Να χρησιμοποιώ πρόγραμμα ασφαλείας					
Να χρησιμοποιώ φίλτρο στο πρόγραμμα περιήγησης για να μπλοκάρει τις κακόβουλες ιστοσελίδες					
Να κρυπτογραφώ όλες τις ευαίσθητες πληροφορίες της εταιρείας					

41. Άλλα σχόλια/ Προτάσεις

Funded by the Erasmus+ Programme of the European Union