ΤΜΗΜΑ ΑΣΦΑΛΕΙΑΣ ΤΡΙΠΟΛΗΣ

ΝΕΟΙ ΜΕΘΟΔΟΙ ΕΞΑΠΑΤΗΣΗΣ ΠΟΛΙΤΩΝ ΚΑΙ ΕΠΙΧΕΙΡΗΣΕΩΝ – ΤΡΟΠΟΙ ΠΡΟΦΥΛΑΞΗΣ

ΕΙΔΗ ΑΠΑΤΩΝ ΕΝΔΕΙΚΤΙΚΑ

- ΙΣΠΑΝΙΚΟ ΛΟΤΤΟ
- ΝΙΓΗΡΙΑΝΗ ΑΠΑΤΗ
- ΑΠΑΤΕΣ ΓΙΑ ΨΕΥΔΕΙΣ ΔΙΑΓΩΝΙΣΜΟΥΣ ΓΙΑ ΔΩΡΟΕΠΙΤΑΓΕΣ ΑΠΟ ΓΝΩΣΤΕΣ ΑΛΥΣΙΔΕΣ ΚΑΤΑΣΤΗΜΑΤΩΝ
- ΑΠΑΤΗ ΓΙΑ ΔΗΘΕΝ ΑΓΟΡΕΣ – ΠΩΛΗΣΕΙΣ ΠΡΟΙΟΝΤΩΝ / ΑΥΤΟΚΙΝΗΤΩΝ
- ΑΠΑΤΑ ΜΕ ΠΡΟΦΑΣΗ ΔΙΑΔΙΚΤΥΑΚΩΝ ΓΝΩΡΙΜΙΩΝ
- SPAMMING
- ΑΠΑΤΗ ΤΗΝ ΠΡΟΦΑΣΗ ΕΠΙΚΟΙΝΩΝΙΑΣ ΜΕ ΛΟΓΙΣΤΗ ΓΙΑ ΤΗΝ ΠΛΗΡΩΜΗ ΕΠΙΔΟΜΑΤΩΝ FUEL PASS – POWER PASS
- PHISHING ΠΡΟΣΩΠΙΚΩΝ ΣΤΟΙΧΕΙΩΝ
- ΑΠΑΤΗ ΜΕΣΩ ΠΛΑΣΤΩΝ ΤΙΜΟΛΟΓΙΩΝ ΚΑΙ ΛΟΙΠΩΝ ΠΑΡΑΣΤΑΤΙΚΩΝ (INVOICE BUSINESS FRAUD)


SCAM

SPAM - SCAMMING

- ΩΣ SPAM ΑΝΑΦΕΡΟΜΑΣΤΕ ΣΤΗΝ ΜΑΖΙΚΗ ΑΠΟΣΤΟΛΗ ΜΗΝΥΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ (EMAIL) ΤΑ ΟΠΟΙΑ ΕΧΟΥΝ ΑΠΡΟΚΛΗΤΟ ΣΥΝΗΘΩΣ ΕΜΠΟΡΙΚΟ ΧΑΡΑΚΤΗΡΑ ΚΑΙ ΑΠΟΣΤΕΛΛΟΝΤΑΙ ΑΔΙΑΚΡΙΤΩΣ
- ΟΤΑΝ Ο ΣΤΟΧΟΣ ΤΟΥ ΑΠΟΣΤΟΛΕΑ ΤΩΝ ΜΗΝΥΜΑΤΩΝ ΕΙΝΑΙ ΝΑ ΕΞΑΠΑΤΗΣΕΙ ΤΩΝ ΑΠΟΔΕΚΤΗ ΚΑΙ ΝΑ ΧΡΗΣΙΜΟΠΟΙΗΣΕΙ ΜΕ ΚΑΚΟΒΟΥΛΟ ΤΡΟΠΟ ΤΑ ΔΕΔΟΜΕΝΑ ΠΟΥ ΘΑ ΥΠΟΚΛΕΨΕΙ ΤΟΤΕ ΕΧΟΥΜΕ ΤΗΝ ΔΙΑΔΙΚΑΣΙΑ SCAMMING.
- Η ΧΡΗΣΗ SMARTPHONE ΑΥΞΗΣΕ ΡΑΓΔΑΙΑ ΤΗΝ ΜΑΖΙΚΗ ΑΠΟΣΤΟΛΗ ΜΗΝΥΜΑΤΩΝ

ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

- ΔΕΝ ΑΝΟΙΓΟΥΜΕ SMAP ΜΗΝΥΜΑΤΑ
- ΔΕΝ ΑΠΑΝΤΑΜΕ ΣΕ SPAM ΜΗΝΥΜΑΤΑ
- ΔΙΑΤΗΡΟΥΜΕ ΑΛΛΟ EMAIL ΓΙΑ ΟΙΚΕΙΟΥΣ ΚΙ ΑΛΛΟ ΓΙΑ ΓΕΝΙΚΗΣ ΧΡΗΣΗΣ ΘΕΜΑΤΑ
- ΠΟΤΕ ΔΕΝ ΑΓΟΡΑΖΟΥΜΕ ΚΑΤΙ ΠΟΥ ΜΑΣ ΑΠΟΣΤΕΛΛΕΤΕ ΜΕΣΩ ΕΝΟΣ ΑΠΟΜΟΝΩΜΕΝΟΥ EMAIL

ΑΠΑΤΗΛΑ ΜΗΝΥΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ (PHISHING)

ΑΠΑΤΗΛΑ ΜΗΝΥΜΑΤΑ SMS (SMISHING)

*Ο όρος **"phishing"** αναφέρεται στα απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου, που σκοπό έχουν να εξαπατηθούν οι παραλήπτες τους και να γνωστοποιήσουν στους απατεώνες **"phishers"** προσωπικές και οικονομικές τους πληροφορίες ή κωδικούς ασφαλείας τους.*

- Ο όρος "smishing" (ένας συνδυασμός των λέξεων "SMS" και "Phishing") αναφέρεται στην προσπάθεια των απατεώνων να αποκτήσουν προσωπικές και οικονομικές πληροφορίες ή κωδικούς ασφαλείας μέσω μηνυμάτων SMS αν και μπορούν να εμφανιστούν σε **οποιαδήποτε πλατφόρμα ανταλλαγής μηνυμάτων** (π.χ. WhatsApp, Instagram Viber κλπ).

Ειδικότερα το Phishing ή αλλιώς «Ψάρεμα» αποτελεί μία τεχνική ηλεκτρονικής απάτης που χρησιμοποιείται από τους εγκληματίες για την απόσπαση προσωπικών στοιχείων οικονομικού χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, κωδικούς taxisnet, βάζοντας ως δόλωμα κάποιο ψεύτικο πρόσχημα.

- Υπάρχουν διάφορες τακτικές που χρησιμοποιούν οι απατεώνες, με τις πιο γνωστές από αυτές να στοχεύουν στο ηλεκτρονικό ταχυδρομείο του θύματος «email».
- Προσποιούμενοι έμπιστες εταιρίες ή τραπεζικά ιδρύματα, ζητούν από το θύμα να τους αποστείλει τα προσωπικά οικονομικά του στοιχεία μέσω e-mail ή να πληκτρολογήσει αυτούς μέσω σε link (υπερσύνδεσμος) που οδηγεί σε πλαστό Site (Τράπεζάς, δημόσιοι οργανισμοί κλπ)
- Οι απατεώνες αξιοποιούν τις πληροφορίες αυτές αποσπώντας χρηματικά ποσά από τις κάρτες ή τους λογαριασμούς των θυμάτων τους

- Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου συνήθως μοιάζουν πάρα πολύ με τα μηνύματα που στέλνουν στους πελάτες τους διάφορες εταιρείες.
- Αντιγράφουν το λογότυπο, τα χαρακτηριστικά και το ύφος των πραγματικών μηνυμάτων ηλεκτρονικού ταχυδρομείου.

- Κάνουν χρήση ορολογίας που δίνει την αίσθηση του κατεπείγοντος.

- **ΣΥΝΗΘΩΣ ΕΧΟΥΝ ΚΑΠΟΙΟ ΟΡΘΟΓΡΑΦΙΚΟ ΛΑΘΟΣ**

- Σας ζητούν να κατεβάσετε στη συσκευή σας ένα επισυναπτόμενο αρχείο ή να κάνετε κλικ σε έναν ηλεκτρονικό σύνδεσμο (link).

- Οι απατεώνες στον κυβερνοχώρο βασίζονται στο γεγονός ότι οι άνθρωποι είναι απασχολημένοι και βιαστικοί.
- Τα απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου (email) αλλά και τα sms μοιάζουν να είναι νόμιμα.
- Ιδιαίτερα όταν χρησιμοποιούμε μια φορητή συσκευή ενδεχομένως να είναι πιο δύσκολο να εντοπίσουμε μια απόπειρα ηλεκτρονικού "ψαρέματος" από το κινητό τηλέφωνο ή το tablet.

ΤΙ ΜΠΟΡΟΥΜΕ ΝΑ ΚΑΝΟΥΜΕ

- Διατηρούμε το λογισμικό ενημερωμένο, περιλαμβανομένου του φυλλομετρητή ιστοσελίδων (browser), του αντιικού προγράμματος (antivirus) και του λειτουργικού συστήματος.
- Είμαστε ιδιαίτερα προσεκτικοί εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου "τράπεζας" μας ζητά ευαίσθητες πληροφορίες (π.χ. τον κωδικό πρόσβασης του τραπεζικού σας λογαριασμού μέσω internet banking).

- Ελέγχουμε προσεκτικά το μήνυμα ηλεκτρονικού ταχυδρομείου ή το sms και συγκρίνουμε τη διεύθυνση με τα προηγούμενα πραγματικά μηνύματα από τον φορέα που φέρεται ότι εστάλη το μήνυμα.
- Ελέγχουμε για ορθογραφικά λάθη και λάθη γραμματικής ή σύνταξης.
- Δεν απαντάμε σε ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου
- Ενημερώνουμε άμεσα την Αστυνομία

- Δεν κάνουμε απευθείας κλικ στον ηλεκτρονικό σύνδεσμο (link) και δεν πραγματοποιούμε λήψη (download) του επισυναπτόμενου αρχείου, αντίθετα πληκτρολογούμε την διεύθυνση του ηλεκτρονικού συνδέσμου στον φυλλομετρητή ιστοσελίδων (browser) που χρησιμοποιούμε.
- Σε περίπτωση οποιασδήποτε αμφιβολίας, ελέγχουμε την ιστοσελίδα ή τηλεφωνούμε στον φερόμενο αποστολέα του μηνύματος (πχ τράπεζα αν το μήνυμα φέρεται ότι εστάλει από τραπεζικό ίδρυμα)

Το μήνυμα κειμένου συνήθως θα μας ζητά να κάνουμε κλικ σε έναν ηλεκτρονικό σύνδεσμο (link) ή να καλέσουμε έναν αριθμό τηλεφώνου, προκειμένου να επαληθεύσουμε, ενημερώσουμε ή επανανεργοποιήσουμε τον λογαριασμό μας. Αλλά...ο ηλεκτρονικός σύνδεσμος οδηγεί σε ψεύτικη ιστοσελίδα και ο αριθμός τηλεφώνου οδηγεί στον απατεώνα που ισχυρίζεται ότι εκπροσωπεί τη νόμιμη επιχείρηση.

Χρειάζεται κάποια ενέργεια από τη μεριά του χρήστη (η απλή λήψη του μηνύματος δεν προκαλεί κάποια ζημιά) **για να μπορέσει να γίνει υποκλοπή των στοιχεία.**

Ποτέ δεν απαντάμε σε μήνυμα κειμένου (sms) που μας ζητά τον κωδικό "PIN" ή τον κωδικό πρόσβασης ("password") στον τραπεζικό σας λογαριασμό ή οποιαδήποτε άλλα εξατομικευμένα διαπιστευτήρια ασφαλείας (π.χ. e-banking user name).

Αγαπητέ πελάτη,
Παρακαλώ να ενημερωθείτε ότι το δέμα σας περιμένει την παράδοση.
Επιβεβαιώστε την πληρωμή 2,99 EUR στον παρακάτω σύνδεσμο.
Σημείωση: η διαδικασία επαλήθευσης πρέπει να γίνει τις επόμενες 02 ημέρες.
Κάντε κλικ στον παρακάτω σύνδεσμο:
https://www.elta.gr/payment

Με εκτιμιση,
Μέλος του Elta Hellenic Post,

From Ελληνικά Ταχυδρομεία <support@podeucentral1route.freshdesk.com> ☆ 1

Subject **το δέμα σας είναι έτοιμο για παράδοση**

To [redacted]

ΕΛΤΑ
Hellenic Post

Αγαπητέ πελάτη, 2

Παρακαλώ να ενημερωθείτε ότι το δέμα σας περιμένει την παράδοση. 3
Επιβεβαιώστε την πληρωμή 2,99 EUR στον παρακάτω σύνδεσμο.
Σημείωση: η διαδικασία επαλήθευσης πρέπει να γίνει τις επόμενες 02 ημέρες. 4
Κάντε κλικ στον παρακάτω σύνδεσμο:
https://www.elta.gr/payment 5

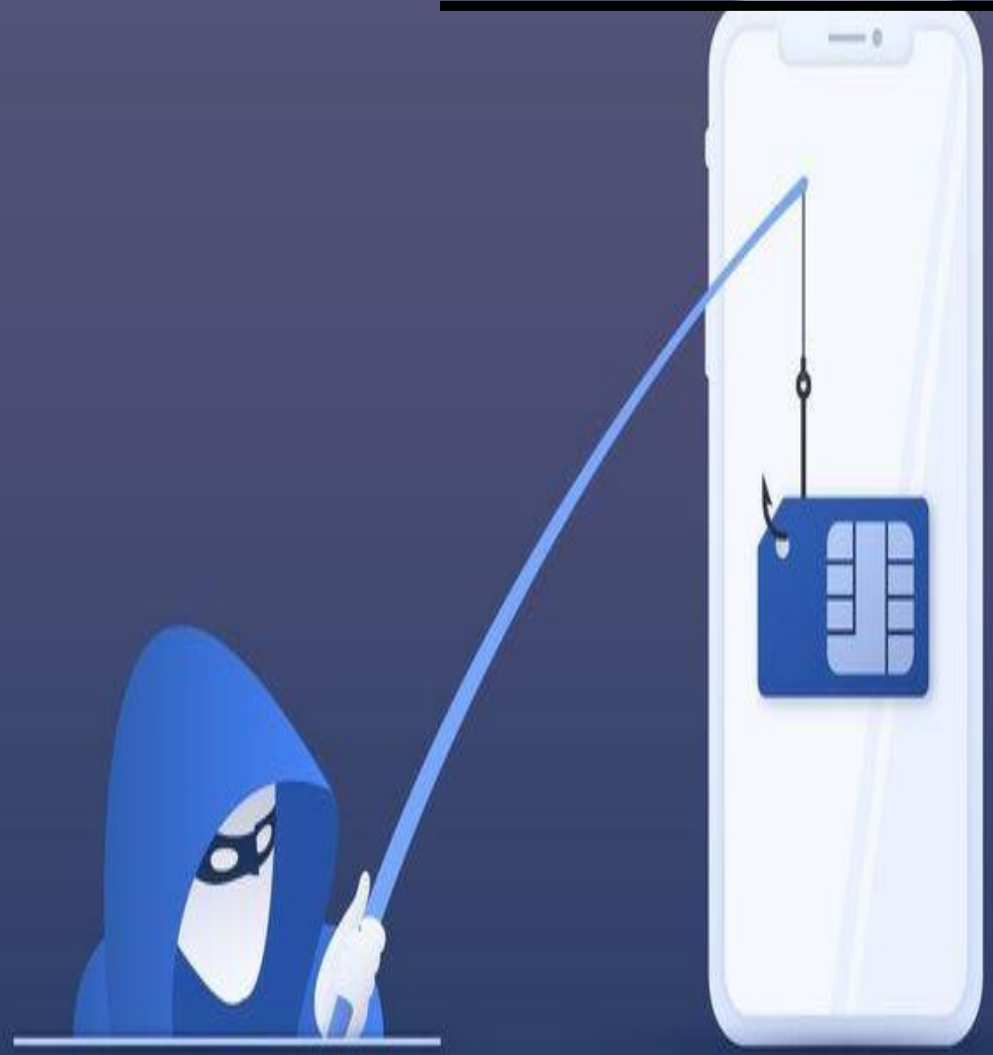
Με εκτιμιση, 6
Μέλος του Elta Hellenic Post, 7

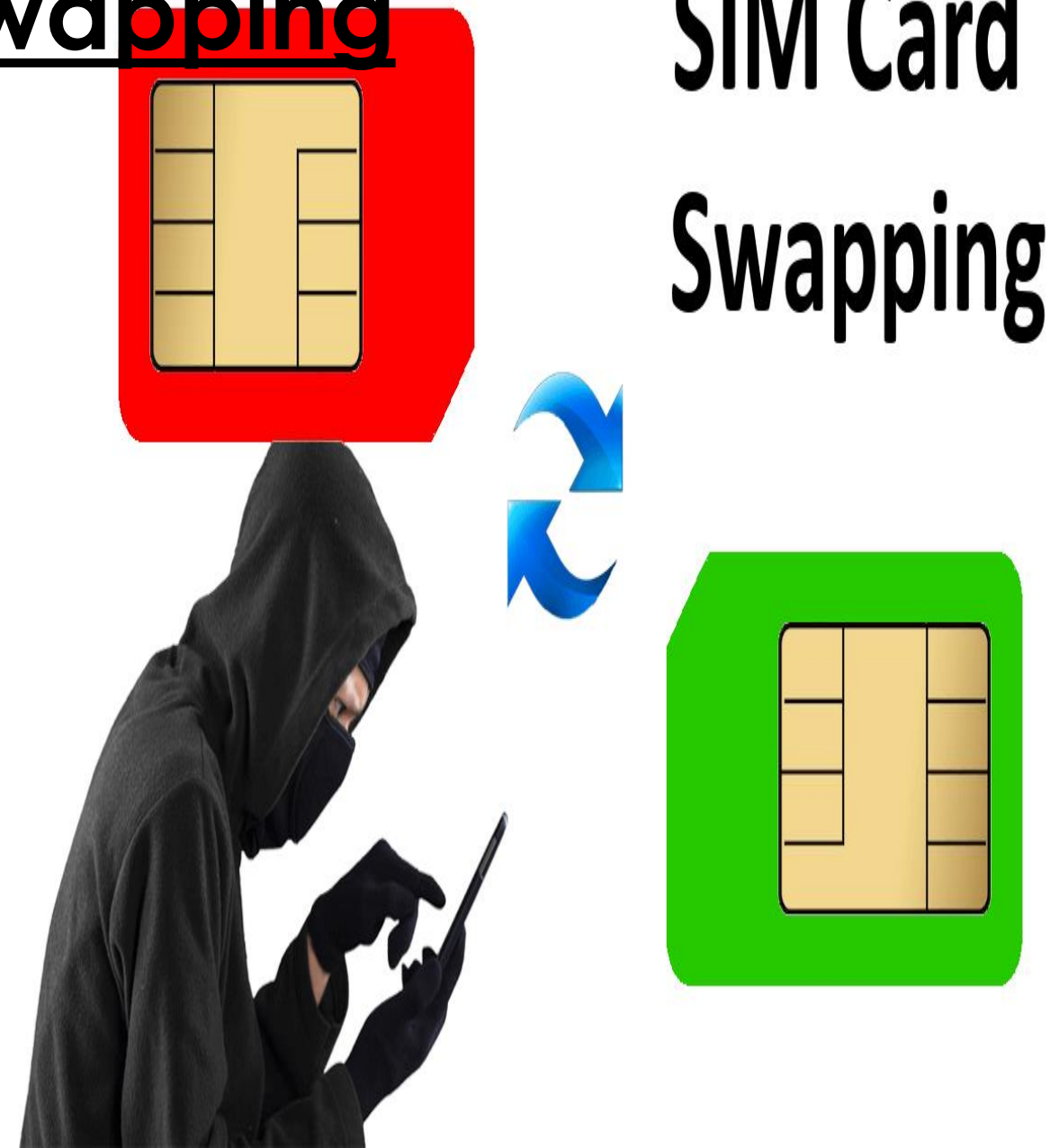
Σημεία που «χτυπάνε καμπανάκι» ότι πρόκειται για απάτη

1. Η ηλεκτρονική διεύθυνση του αποστολέα **δεν μοιάζει να είναι τα Ελληνικά Ταχυδρομεία** γιατί φαίνεται να είναι το → support@podeucentral1route.freshdesk.com.
2. **Δεν αναφέρει το όνομα σας,** γιατί το μήνυμα αυτό είναι αυτοματοποιημένο και οι απατεώνες δεν ξέρουν ποιοι είσαστε παρά μόνο το e-mail σας.
3. Σας ζητάει **χρήματα**. Φαίνεται μικρό ποσό για να για να μην κινήσει υποψίες και αποκαλυφθεί η απάτη.
4. Δίνει την αίσθηση του **επείγοντος** για να αγχωθείτε και να μην σας αφήσει αυτό να σκεφτείτε με ψυχραιμία.
5. Σας εμφανίζει ένα e-mail που **μοιάζει με mail των ΕΛΤΑ** , αλλά αν βάλετε το ποντίκι πάνω στην διεύθυνση αυτή (όχι να πατήσετε αλλά να αιωρείστε το ποντίκι του υπολογιστή σας) θα εμφανιστεί **η πραγματική διεύθυνση** στην οποία θα σας στείλει το link, η οποία **δεν είναι αυτή που φαίνεται στο e-mail** . Η πραγματική διεύθυνση είναι αυτή που θα σας εμφανιστεί κάτω αριστερά στον υπολογιστή σας και είναι η → https://www.gruppolimpiantistica.com/video/gr/.
6. Έχει ορθογραφικά λάθη. Συγκεκριμένα η λέξη «**εκτίμηση**» είναι λάθος γραμμένη και λείπουν και τόνοι.
7. **Δεν υπάρχει υπογραφή συγκεκριμένου ατόμου από τα ΕΛΤΑ**, μόνο κάποια γενική περίεργη υπογραφή.

((•)) https://www.gruppolimpiantistica.com/video/gr/ 5

ΑΠΑΤΗ SIM Swapping





Στις περιπτώσεις απάτης τύπου SIM Swapping, **οι δράστες εκμεταλλεύονται τη δυνατότητα αλλαγής κάρτας SIM και προσποιούνται είτε τον κάτοχο της κάρτας SIM ή κάποιον εξουσιοδοτημένο από τον νόμιμο συνδρομητή**, προσπαθώντας έτσι να εξαπατήσουν τους παρόχους κινητής τηλεφωνίας και να αποκτήσουν νέα κάρτα προς αντικατάσταση αυτής που έχει ο νόμιμος κάτοχος.

Μόλις ενεργοποιήσουν τη νέα κάρτα, η παλιά, που βρίσκεται στην κατοχή του νόμιμου συνδρομητή, απενεργοποιείται και έτσι όλες οι υπηρεσίες (κλήσεις, SMS, πρόσβαση στο διαδίκτυο) λαμβάνονται στη συσκευή που βρίσκεται στην κατοχή του εξαπατήσαντος δράστη, δίνοντάς τους τη δυνατότητα να διεξάγουν παράνομες δραστηριότητες εν αγνοία των νόμιμων συνδρομητών (π.χ. λαμβάνοντας κλήσεις και μηνύματα που προορίζονται για αυτούς, υποκλέπτοντας κωδικούς μιας χρήσης ή μηνυμάτων επαλήθευσης ασφάλειας κ.λ.π.).

Η μη εξουσιοδοτημένη αντικατάσταση/ανταλλαγή της κάρτας SIM αποτελεί συνήθως το δεύτερο σκέλος του παραπάνω παράνομου τρόπου δράσης.

Κατά το πρώτο σκέλος, οι δράστες έχουν καταφέρει να υποκλέψουν τους κωδικούς e-Banking συνήθως μέσω ενός ηλεκτρονικού μηνύματος «ψαρέματος» (phishing) ή μέσω κακόβουλου λογισμικού (trojan /malware) που έχουν εγκαταστήσει στον υπολογιστή του θύματος.

ΤΙ ΜΠΟΡΕΙΣ ΝΑ ΚΑΝΕΙΣ

Αν το κινητό σταματήσει να λειτουργεί για ασυνήθιστους λόγους, επικοινωνούμε αμέσως με τον πάροχο κινητής τηλεφωνίας. Μερικές φορές μπορεί να χάσουμε το σήμα λόγω ευρύτερων προβλημάτων που επηρεάζουν την υπηρεσία κινητής τηλεφωνίας. Ωστόσο, εάν χάσουμε την υπηρεσία σε μια θέση που συνήθως έχει καλή κάλυψη, είναι ασφαλέστερο να επικοινωνήσουμε με τον πάροχο του δικτύου και να επιβεβαιώσουμε ότι δεν έχει απενεργοποιηθεί η SIM.

- **Δεν αποκαλύπτουμε τον αριθμό του κινητού τηλεφώνου στα μέσα κοινωνικής δικτύωσης.**
- **Ενεργοποιούμε το ιδιωτικό απόρρητο στα μέσα κοινωνικής δικτύωσης**
- Κάνουμε εγγραφή στις υπηρεσίες των οργανισμών που παρέχουν **ειδοποιήσεις SMS** και ηλεκτρονικού ταχυδρομείου **όταν εκτελούνται συναλλαγές.**
- **Δεν απαντάμε ποτέ σε άγνωστα μηνύματα ή κλήσεις που μας ζητούν τα στοιχεία λογαριασμών** και τον καταχωρημένο αριθμό του κινητού τηλεφώνου.

ΑΠΑΤΗ ΜΕΣΩ ΠΛΑΣΤΩΝ ΤΙΜΟΛΟΓΙΩΝ ΚΑΙ ΛΟΙΠΩΝ ΠΑΡΑΣΤΑΤΙΚΩΝ (INVOICE BUSINESS FRAUD)

- Μια επιχείρηση προσεγγίζεται από κάποιον τρίτο που ισχυρίζεται ότι εκπροσωπεί έναν προμηθευτή/πάροχο υπηρεσιών/δικαιούχο μιας πληρωμής.

- Μπορεί να γίνει χρήση συνδυασμού πρακτικών προσέγγισης: τηλέφωνο, επιστολή, e-mail, κ.λπ

Ο απατεώνας ζητάει να τροποποιηθούν οι πληροφορίες για τις μελλοντικές πληρωμές τιμολογίων (δηλαδή τα στοιχεία του τραπεζικού λογαριασμού του δικαιούχου πληρωμής). Ο νέος προτεινόμενος λογαριασμός ανήκει στον απατεώνα.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ ΩΣ ΕΠΙΧΕΙΡΗΣΗ

- Διασφαλίστε ότι οι υπάλληλοι είναι ενημερωμένοι και γνωρίζουν τη συγκεκριμένη μορφή απάτης και τον τρόπο αποφυγής της.
- Εφαρμόστε διαδικασία για την επαλήθευση της νομιμότητας των αιτημάτων πληρωμής που λαμβάνετε.
- Ελέγξτε τις πληροφορίες που αναρτώνται στην ιστοσελίδα της επιχείρησής σας και συγκεκριμένα τα συμβόλαια και τους προμηθευτές σας. Διασφαλίστε ότι το προσωπικό περιορίζει τη γνωστοποίηση πληροφοριών της επιχείρησης στα μέσα κοινωνικής δικτύωσης.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ ΩΣ ΥΠΑΛΛΗΛΟΣ

- Επαληθεύστε ότι όλα τα αιτήματα πληρωμών προέρχονται από τους πραγματικούς προμηθευτές της επιχείρησης, ειδικά εάν σας ζητούν να τροποποιήσετε τα στοιχεία των τραπεζικών τους λογαριασμών για τις μελλοντικές πληρωμές των τιμολογίων ή λοιπών παραστατικών.
- Για πληρωμές που υπερβαίνουν ένα συγκεκριμένο όριο ποσού, καθορίστε μια διαδικασία για την επιβεβαίωση του ορθού τραπεζικού λογαριασμού και του αποδέκτη (π.χ. επικοινωνία με την επιχείρηση)
- Περιορίστε τις πληροφορίες που γνωστοποιείτε για τον εργοδότη σας στα μέσα κοινωνικής δικτύωσης

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ ΩΣ ΥΠΑΛΛΗΛΟΣ

- Μην κάνετε χρήση των στοιχείων επικοινωνίας που περιλαμβάνονται στην επιστολή/fax/e-mail στο οποίο ζητείται η αλλαγή στοιχείων. Αντίθετα, χρησιμοποιείστε τα στοιχεία επικοινωνίας από την προηγούμενη αλληλογραφία σας με τον προμηθευτή.
- Όταν πληρώνετε ένα τιμολόγιο, να στέλνετε e-mail ενημέρωσης του αποδέκτη της πληρωμής. Σε αυτό να γράφετε την επωνυμία της τράπεζάς του και τα τέσσερα τελευταία ψηφία του τραπεζικού του λογαριασμού για τη διασφάλιση της συναλλαγής.

ΜΙΑ ΠΑΥΣΗ ΑΡΚΕΙ

ΓΙΑ ΝΑ ΑΠΟΦΥΓΟΥΜΕ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΑΠΑΤΗ

- ΤΗΛΕΦΩΝΑ ΕΠΙΚΟΙΝΩΝΙΑΣ
- ΔΙΟΙΚΗΤΗΣ: 2710230514 / 2710222549
- ΑΞΙΩΜΑΤΙΚΟΣ ΥΠΗΡΕΣΙΑΣ : 2710230560
- ΑΞΙΩΜΑΤΙΚΟΙ: 2710230557