Η προστασία της κοινωνίας από την ανάπτυξη νέων μορφών τεχνολογίας

της **ΑΝΝΑΣ ΓΑΡΥΦΑΛΛΗ**
Στελέχους του Τομέα Συστημάτων Πληρωμών και Ηλεκτρονικής Τραπεζικής της ΕΕΤ

Παρόλο που η τεχνολογία προσφέρει τεράστια πλεονεκτήματα και μεγάλες ευκαιρίες, η χρήση της συνεπάγεται και διάφορους κινδύνους. Έχοντας αυτό κατά νου, οι τράπεζες λαμβάνουν εκτεταμένα μέτρα για να προστατεύσουν τις πληροφορίες που μεταβιβάζονται και διεκπεραιώνονται κατά τη διενέργεια των ηλεκτρονικών τραπεζικών συναλλαγών.

1. Απειλές που συνδέονται με τη χρήση του διαδικτύου

Δεδομένης της δυσκολίας να «αλωθούν» τα τραπεζικά συστήματα λόγω των πολλαπλών επιπέδων ασφάλειας, οι επίδοξοι κακοποιοί αναπόφευκτα στρέφονται προς πιο ευάλωτους στόχους, όπως είναι οι απλοί χρήστες του διαδικτύου.

Εκ των πραγμάτων, οι τράπεζες δεν είναι σε θέση να ασκήσουν έλεγχο στα συστήματα που χρησιμοποιούν οι πελάτες τους για τις τραπεζικές τους συναλλαγές στο διαδίκτυο. Επιπλέον, αυτά τα συστήματα – λόγου χάρη ένας προσωπικός υπολογιστής συνδεδεμένος στο διαδίκτυο – συνήθως χρησιμοποιούνται και για διάφορες άλλες εφαρμογές, με συνέπεια την έκθεσή τους σε πολλαπλούς κινδύνους που είναι δύσκολο να ελεγχθούν.

Οι σοβαρότερες και συνηθέστερες απειλές που συνδέονται με τη χρήση του διαδικτύου σήμερα είναι οι εξής:

- Hacking: μη εξουσιοδοτημένη πρόσβαση στον υπολογιστή του χρήστη μέσω του διαδικτύου, με αποτέλεσμα την υποκλοπή, παραποίηση ή διαγραφή των μεταβιβαζόμενων πληροφοριών.

- Ιοί και worms: προγράμματα που αναπαράγονται από μόνα τους ή αποστέλλονται μέσω διαδικτύου με e-mail και μπορούν να καταστρέψουν αρχεία ή δεδομένα του υπολογιστή.
- Trojan (δούρειοι ίπποι) ή key loggers, spy ware: προγράμματα που, χωρίς να το γνωρίζει ο χρήστης, εκτελούν εργασίες οι οποίες θέτουν σε κίνδυνο την ασφάλεια του υπολογιστή, όπως η υποκλοπή κωδικών πρόσβασης.
- Phishing: διόδευση των ανυποψίαστων χρηστών προς παραπλανητικές ιστοσελίδες-παγίδες με σκοπό την απόσπαση προσωπικών και εμπιστευτικών πληροφοριών.

Οι τράπεζες λαμβάνουν συνεχώς μέτρα, τα οποία εξασφαλίζουν ουσιαστική προστασία των συστημάτων τους από απευθείας επιθέσεις εναντίον τους. Θα πρέπει όμως να λαμβάνουν και οι χρήστες/πελάτες των τραπεζών κάποια μέτρα για την προστασία των δικών τους συστημάτων.

Ακολουθώντας τους 10 κανόνες που περιγράφονται στη συνέχεια, οι χρήστες μπορούν να ενισχύσουν σημαντικά την ασφάλεια του υπολογιστή που χρησιμοποιούν για την πρόσβασή τους στο διαδίκτυο και να περιορίσουν τους κινδύνους στο ελάχιστο.

1.	Προστατεύστε τα απόρρητα προσωπικά δεδομένα που στέλνετε μέσω διαδικτύου.
2.	Βεβαιωθείτε για την ταυτότητα αυτού με τον οποίο επικοινωνείτε.
3.	Μην αποθηκεύετε απόρρητα προσωπικά δεδομένα στο σκληρό δίσκο υπολογιστή που δεν χρησιμοποιείται μόνο από εσάς.
4.	Επιλέξτε ασφαλή κωδικό πρόσβασης.
5.	Χρησιμοποιείτε προγράμματα μόνο από αξιόπιστες πηγές.
6.	Χρησιμοποιείτε ενημερωμένες εκδόσεις προγραμμάτων.
7.	Εκτελέστε έλεγχο ασφαλείας στον υπολογιστή σας.
8.	Ενεργοποιείστε τις ρυθμίσεις ασφαλείας του προγράμματος πλοήγησης.
9.	Εγκαταστήστε προγράμματα ανίχνευσης ιών και πρόσθετο λογισμικό ασφαλείας.
10.	Δημιουργείτε τακτικά αντίγραφα ασφαλείας.

Η ΕΕΤ, σχετικά με το δεύτερο κανόνα, σύμφωνα με τον οποίο δεν πρέπει να γνωστοποιούμε προσωπικά δεδομένα μας αν δεν είμαστε βέβαιοι ποιος τα λαμβάνει, και σε συνδυασμό με την αντιμετώπιση κρουσμάτων αποστολής πλαστών ηλεκτρονικών μηνυμάτων (phishing e-mail)[1] με σκοπό την υποκλοπή προσωπικών δεδομένων χρηστών υπηρεσιών ηλεκτρονικής τραπεζικής των τραπεζών, επισημαίνει στους χρήστες τα εξής:

- **Αγνοήστε e-mail στα οποία ζητούνται προσωπικά σας στοιχεία (αριθμός λογαριασμού, μυστικοί προσωπικοί κωδικοί, ονοματεπώνυμο κ.ά.).**

  Οι τράπεζες δεν πρόκειται για κανένα λόγο να σας ζητήσουν τα προσωπικά σας στοιχεία μέσω e-mail ή τηλεφώνου. Για το λόγο αυτό να διαγράφετε τα e-mail αυτά ως πλαστά και να αγνοείτε αντίστοιχες πιθανές τηλεφωνικές κλήσεις.

  Σε περίπτωση που έχετε λάβει πλαστό e-mail και έχετε ήδη απαντήσει παρέχοντας προσωπικά σας στοιχεία, επικοινωνήστε άμεσα με την τράπεζά σας και ακολουθήστε τις οδηγίες που θα σας δοθούν.

- **Μην εισάγετε τους μυστικούς προσωπικούς κωδικούς σας, αν δεν βεβαιωθείτε πριν ότι βρίσκεστε στη σωστή διεύθυνση της τράπεζάς σας.** Πληκτρολογήστε εσείς τη διεύθυνση της ιστοσελίδας της τράπεζας που θέλετε να επισκεφθείτε. Μη συνδέεστε ποτέ μέσω εξωτερικού συνδέσμου (link).

- **Βεβαιωθείτε ότι στην ιστοσελίδα ηλεκτρονικής τραπεζικής της τράπεζάς σας εμφανίζεται κάτω δεξιά και το εικονίδιο με το «λουκέτο»**  μέσω του οποίου μπορείτε, ανοίγοντάς το με διπλό κλικ, να επιβεβαιώσετε ότι βρίσκεστε στο ασφαλές περιβάλλον της τράπεζάς σας.

- **Ενημερωθείτε για τους γενικότερους κανόνες ασφάλειας των συναλλαγών** από την υπηρεσία ηλεκτρονικής τραπεζικής της τράπεζάς σας.

Οι τράπεζες έχουν λάβει όλα τα απαραίτητα μέτρα για τη διασφάλιση των συναλλαγών σας. Η τήρηση όμως του απορρήτου των προσωπικών σας στοιχείων είναι αποκλειστικά δική σας υπόθεση.

2. Απειλές που συνδέονται με τη χρήση των καρτών

2.1. Έκδοση καρτών με πλαστά στοιχεία ταυτότητας και πλαστά εκκαθαριστικά εφορίας (identity fraud)

Το είδος αυτό της απάτης γνωστό και σαν identity theft αυξάνεται συνεχώς. Οι μέχρι τώρα ενέργειες που έχουν γίνει είναι οι εξής:

[1] *Phishing*: Απάτη στο πλαίσιο της οποίας λαμβάνετε ένα e-mail που δίνει την εντύπωση ότι προέρχεται από την τράπεζά σας. Το e-mail σας ζητά να μεταβείτε στην ιστοσελίδα της τράπεζάς σας και να ανανεώσετε τους κωδικούς πρόσβασής σας. Όμως η σύνδεση (link) που εμφανίζεται στο e-mail θα σας μεταφέρει σε μια παρόμοια ιστοσελίδα, κατασκευασμένη από τον απατεώνα, ο οποίος θα είναι πλέον σε θέση να υποκλέψει τους μυστικούς κωδικούς που καλοπροαίρετα θα δώσετε.

- Συνεργασία ΕΕΤ και Ελληνικής Αστυνομίας όσον αφορά τα χαρακτηριστικά ασφαλείας των εγγράφων ταυτοποίησης, με τα οποία οι πολίτες προσέρχονται στις τράπεζες, όπως ταυτότητες, διαβατήρια, στρατιωτικές ταυτότητες κ.λπ., ώστε να ενημερωθούν υπεύθυνα και κατάλληλα τα στελέχη των τραπεζών.
- Δημιουργία ενημερωτικού υλικού με συνεργασία της ΕΕΤ, της Ελληνικής Αστυνομίας και της ΤΕΙΡΕΣΙΑΣ ΑΕ («Οδηγίες προς τους πολίτες σε περίπτωση κλοπής ή απώλειας αστυνομικής ταυτότητας ή διαβατηρίου»), όπου δίνονται οδηγίες προς τους πολίτες σχετικά με το θέμα. Το υλικό έχει δοθεί στις τράπεζες, καθώς και σε άλλους φορείς (Υπουργείο Εσωτερικών, Υπουργείο Δημόσιας Τάξης, Τραπεζικό Μεσολαβητή, Ενώσεις Καταναλωτών, Σωματεία Εργαζομένων) προς αξιοποίηση.

2.2. Κλοπή και απατηλή χρήση καρτών

Το είδος αυτό της απάτης οφείλεται κυρίως στις πιο κάτω αιτίες:

2.2.1. Κλοπή ή απώλεια των καρτών που έχει ο νόμιμος κάτοχος στο πορτοφόλι του.

Ο κλέφτης φροντίζει να πραγματοποιεί με τις πιστωτικές κάρτες, συναλλαγές μικρής αξίας σε επιχειρήσεις, ώστε να μη χρειάζεται η λήψη εξουσιοδότησης από τον εκδότη και συνήθως τις πρώτες ώρες από την κλοπή. Ο κάτοχος δεν πρέπει ποτέ να έχει μαζί με την κάρτα και το PIN του, καθώς έτσι κινδυνεύει να του πάρει ο κλέφτης και χρήματα από το λογαριασμό του. Ο νόμιμος κάτοχος οφείλει να ειδοποιεί, αμέσως μόλις αντιληφθεί το συμβάν, την τράπεζά του και επιπλέον να κάνει δήλωση κλοπής ή απώλειας στην Αστυνομία.

2.2.2. Κλοπή των καρτών που αποστέλλουν οι τράπεζες ταχυδρομικώς στους πελάτες τους.

Το είδος αυτό της απάτης συμβαίνει με την κλοπή των φακέλων σε πολυκατοικίες. Οι τράπεζες ποτέ δεν αποστέλλουν το PIN μαζί με την κάρτα και πολλές τράπεζες έχουν εγκαταστήσει ηλεκτρονικά συστήματα παρακολούθησης της χρήσης των καρτών των πελατών τους. Αν παρατηρήσουν ασυνήθιστη χρήση ειδοποιούν τηλεφωνικά τον πελάτη τους, προκειμένου να εξακριβώσουν αν όντως έχει πραγματοποιήσει τις σχετικές συναλλαγές.

2.2.3. Υποκλοπή των περιεχομένων της μαγνητικής πίστας των καρτών και του PIN (skimming) και πραγματοποίηση συναλλαγών με πλαστογραφημένες κάρτες.

Είναι η πιο διαδεδομένη απάτη στα ΑΤΜ. Πραγματοποιείται με την εγκατάσταση ειδικών ηλεκτρονικών μηχανισμών και μικροκαμερών στα ΑΤΜ των τραπεζών, τα οποία είναι πολύ δύσκολο να εντοπίσει ο πελάτης και στοχεύουν στην αντιγραφή των περιεχομένων της μαγνητικής πίστας των καρτών και την υποκλοπή του PIN.

Οι κάρτες που έχουν «διαβαστεί» από το ειδικό εξάρτημα (skimmer) μπορούν αργότερα να αναπαραχθούν από τους δράστες στο «εργαστήριό τους».

Σε πολλές περιπτώσεις τα στοιχεία της κάρτας μεταδίδονται σε πραγματικό χρόνο σε κάποιο παραπλήσιο αυτοκίνητο ή μηχανή με κατάλληλο εξοπλισμό ώστε η επεξεργασία τους να γίνεται αμέσως από τους δράστες.

Για την αντιμετώπιση αυτού του είδους της απάτης, οι τράπεζες έχουν προβεί στις εξής ενέργειες:

- Προχωρούν, με επενδύσεις εκατομμυρίων ευρώ, στον εφοδιασμό των καρτών τους με chip, το οποίο θα φέρει τις προδιαγραφές ασφαλείας EMV. Η αλλαγή όλων των καρτών θα έχει ολοκληρωθεί μέχρι το 2010. Η επένδυση αυτή καθιστά αδύνατη την αντιγραφή του περιεχομένου του chip, στο οποίο και θα φυλάσσονται οι πληροφορίες για την κάρτα του κατόχου. Το chip θα επιτρέπει και τη χρήση PIN και για συναλλαγές με επιχειρήσεις που δεν είναι συνδεδεμένες on-line με την τράπεζα που εξέδωσε την κάρτα.
- Έχουν εκδώσει φυλλάδιο με τίτλο *«Συναλλαγές στα ΑΤΜ, γρήγορα και απλά.... αλλά όχι στα τυφλά...»*, το οποίο παρέχει συμβουλές στους συναλλασσομένους για την ενίσχυση της ασφάλειάς τους κατά τη χρήση των καρτών τους στα ΑΤΜ. Το περιεχόμενο του διατραπεζικού φυλλαδίου δημοσιεύτηκε επανειλημμένα στον ημερήσιο Τύπο.
- Έχουν αναπτύξει στενή συνεργασία με την Αστυνομία και την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) για την καταπολέμηση του skimming στα ΑΤΜ.
- Οργάνωσαν ημερίδες, στις οποίες κλήθηκαν οι εκπρόσωποι των εταιρειών που εμπορεύονται στη χώρα μας τα ΑΤΜ, αλλά και εταιρειών από το εξωτερικό, προκειμένου να παρουσιάσουν στους εκπροσώπους των τραπεζών τους μηχανισμούς προστασίας που έχουν κατασκευάσει για την αποφυγή της απάτης στα ΑΤΜ.
- Έχουν στενή συνεργασία και εκπροσωπούνται στην επιτροπή European ATM Security Team, η οποία είναι μονάδα της EUROPOL, ασχολείται με την απάτη στα ΑΤΜ πανευρωπαϊκά και συνεδριάζει στη Χάγη κάθε τρίμηνο.

2.2.4. Αντιγραφή των στοιχείων των καρτών, όπως αυτά αποτυπώνονται στις αποδείξεις των συναλλαγών

Για την αντιμετώπιση αυτού του είδους απάτης, το οποίο πραγματοποιείται συνήθως με τη σύμπραξη υπαλλήλων ή ιδιοκτητών επιχειρήσεων, οι τράπεζες έχουν προχωρήσει στις εξής ενέργειες:

- Σε συνεργασία με την ΤΕΙΡΕΣΙΑΣ ΑΕ έχουν δημιουργήσει μία βάση πληροφοριών, στην οποία καταχωρούνται οι επιχειρήσεις των οποίων έχει καταγγελθεί η σύμβαση αποδοχής με κάρτες.
- Μετέχουν ενεργά στην πρωτοβουλία της Card Fraud Prevention Task Force του Ευρωπαϊκού Συμβουλίου Πληρωμών για τη δημιουργία Πανευρωπαϊκής Βάσης Δεδομένων, στην οποία θα καταχωρούνται, με φροντίδα των ευρωπαϊκών τραπεζών που εκδίδουν κάρτες πληρωμών, τα στοιχεία των επιχειρήσεων στις οποίες παρατηρούνται κρούσματα απάτης (συναλλαγές) με κάρτες.

2.2.5. Εξαπάτηση των κατόχων καρτών, κυρίως μέσω του internet, για την υποκλοπή των απόρρητων προσωπικών τους πληροφοριών, όπως ο PIN (phishing, αντιγραφή πληκτρολόγησης)

Οι τράπεζες ενημερώνουν τους πελάτες τους ότι θα πρέπει να διαθέτουν σύστημα antivirus του υπολογιστή τους και να το ενημερώνουν, ότι δεν πρέπει σε καμία περίπτωση να δίνουν τα προσωπικά και οικονομικά τους στοιχεία σε τρίτους που εμφανίζονται σαν εκπρόσωποι των τραπεζών ή τους υπόσχονται διάφορα χρηματικά ποσά, να μην ανοίγουν e-mails από άγνωστους αποστολείς και να μην μεταβαίνουν σε ιστοσελίδες που τους προτείνονται από διάφορα e-mails.

Σε κάθε περίπτωση οι πελάτες *πρέπει να ελέγχουν προσεκτικά το λογαριασμό της κάρτας τους και να ενημερώνουν άμεσα την τράπεζα για συναλλαγές που αμφισβητούν.*

Η σημερινή εποχή της Κοινωνίας της Πληροφορίας ενσωματώνει στην καθημερινότητά της, τεχνολογίες πληροφοριών και επικοινωνιών, οι οποίες, παρότι μπορεί να ενέχουν κινδύνους, βοηθούν στη βελτίωση και διευκόλυνσή της.

Οι τράπεζες, οι οποίες είναι πρωτοπόροι στην υιοθέτηση των νέων τεχνολογιών, δίνουν ιδιαίτερη σημασία στην ασφάλεια των ηλεκτρονικών συναλλαγών και λαμβάνουν όλα τα απαραίτητα μέτρα για τη θωράκιση της πληροφοριακής υποδομής τους, χρησιμοποιώντας τις πιο σύγχρονες μεθόδους.