ΔΗΜΟΣ ΜΕΓΑΡΕΩΝ
ΟΔΗΓΟΣ
ΨΗΦΙΑΚΗΣ
ΑΣΦΑΛΕΙΑΣ
Γραφείο Επικοινωνίας & Δημοσίων Σχέσεων
Ιανουάριος 2022

Σημείωμα του Δημάρχου

Ο διάσημος χάκερ Κέβιν Μίτνικ είπε κάποτε οτι «οι εταιρείες ξοδεύουν εκατομμύρια σε προγράμματα για ασφάλεια αλλά είναι πεταμένα λεφτά: δεν αντιμετωπίζουν τον πιο αδύναμο κρίκο στην αλυσίδα της ασφάλειας». Εννοούσε βέβαια τους ανθρώπους, αφού αυτοί χειρίζονται τους υπολογιστές και ευθύνονται για τις πληροφορίες που απαιτούν προστασία.

Στο πλαίσιο της ψηφιοποίησης του Δήμου, η ασφάλεια των πληροφοριών και η σχετική εκπαίδευση του προσωπικού είναι ψηλά στη λίστα των δράσεων που σχεδιάζουμε. Έτσι, μετά το Δεκάλογο Ψηφιακής Ασφάλειας, που αναπτύξαμε και εφαρμόζουμε πιλοτικά από την αρχή του χρόνου, ετοιμάσαμε το φυλλάδιο αυτό που μας εισάγει στην έννοια της ασφάλειας, ειδικά τους λιγότερο εξοικειωμένους από εμάς.

Ζήτησα να διατεθεί δωρεάν σε όλους τους συμπολίτες μας, σε μια προσπάθεια περιορισμού της τεχνοφοβίας και του ψηφιακού αναλφαβητισμού.

Όπως λένε για τα βιβλία, καλοτάξιδο!

Γρηγόρης Σταμούλης
Αντιστράτηγος ε.α.
Δήμαρχος Μεγαρέων

Λάβατε e-mail με προσφορά για ένα απίστευτα φθηνό πακέτο διακοπών;
Κάποιος θελει να σας χαρίσει ή δανείσει εκατομμύρια;
Σας ζητούν άγνωστοι να εγκαταστήσετε κάποιο λογισμικό “για την ασφάλειά σας”;
Λάβατε SMS ή e-mail όπου σας κατηγορούν για κάτι για το οποίο δε γνωρίζετε τίποτα;
Σας προσφέρουν κάποια βοήθεια χωρίς να την έχετε ζητήσει;
Σας ζητούν να κάνετε κάτι “κατεπειγόντως”, πχ να καλέσετε έναν αριθμό;
Κάποιος προσπαθεί να σας πανικοβάλει στο τηλέφωνο ή στο e-mail;
Σας ζητούν πληροφορίες ή ταυτοποίηση στοιχείων, αλλά κάλεσαν εκείνοι κι όχι εσείς;
Καλεί κάποιος που γνωρίζει ορισμένα στοιχεία σας και ζητάει περισσότερα “για επαλήθευση”;

Τα παραπάνω είναι ορισμένες από τις απάτες της ψηφιακής εποχής.
Στον οδηγό αυτό θα μάθετε να τις αναγνωρίζετε και, ως ένα βαθμό, να τις αντιμετωπίζετε.

ΓΡΑΦΕΙΟ ΕΠΙΚΟΙΝΩΝΙΑΣ & ΔΗΜΟΣΙΩΝ ΣΧΕΣΕΩΝ
ΔΗΜΟΣ ΜΕΓΑΡΕΩΝ

Περιεχόμενα

I. Πρόλογος....5
II. Η έννοια της ασφάλειας....6
Εκτίμηση κινδύνου σε υπολογιστικά συστήματα....7
III. Ορισμοί και Διαδικασίες....8
1. Καταγραφή και αξιολόγηση....8
2. Διασφάλιση....8
3. Τυποποίηση....8
4. "Ευαίσθητες" πληροφορίες από το internet....9
5. Ασφάλεια πολλών επιπέδων....9
Επίπεδα ελέγχου-προστασίας....9
Χαρακτηρισμός δεδομένων....10
Έλεγχος πρόσβασης....10
Διασφάλιση με τεχνικά μέσα....10
Αντίγραφα ασφαλείας....10
6. Σε περίπτωση παραβίασης....10
IV. Πρακτικά Παραδείγματα....11
1. Κοινωνική μηχανική....11
2. Πλαστοπροσωπία (fraud)....12
3. Ψάρεμα (phishing)....12
4. Απατηλή προστασία....13
5. Κακόβουλο λογισμικό....13
6. Adware – Spyware....13
7. Email....14
7.1 Εκφοβισμός Αρχής....14
7.2 Φιλική Προσέγγιση....14
7.3 Λάθος Παραγγελίας....14
7.4 Σύντομα Λήγει....14
7.5 Εντοπισμός Παραβίασης....14
7.6 Μοναδικός Νικητής....15
7.7 Τραπεζική Ενημέρωση....15
7.8 Θυματοποίηση....15
7.9 Εφορία....15
7.10 Επαλήθευση Στοιχείων....15
7.11 Αναβάθμιση Υπηρεσίας....16
Τί κάνω τώρα;....16
8. Κινητά....17
8.1 Αναπάντητες Κλήσεις....17
8.2 Τηλεφωνικό Phishing (Vishing)....17
8.3 SMS Phishing (Smishing)....17
8.4 Ηχογραφημένα Μηνύματα....17
8.5 Ήχοι Κλήσεων....17
8.6 Ασφάλεια Τηλεφώνου....18
Καλές πρακτικές στο κινητό....18

Οδηγός Ψηφιακής Ασφάλειας

Εγχειρίδιο για την ασφαλέστερη χρήση υπολογιστή και την προστασία από συνήθεις ηλεκτρονικές απειλές και απάτες.

Ι. Πρόλογος

Σκοπός του οδηγού αυτού είναι η εισαγωγή του αναγνώστη στην έννοια της ψηφιακής ασφάλειας (cyber security) και η βασική εκπαίδευσή του στην αξιολόγηση και διαχείριση των πιθανότερων απειλών για τις πληροφορίες, για τον ίδιο σαν άτομο και, εντέλει, για το Δήμο και τις υπηρεσίες του. Ο οδηγός απευθύνεται κυρίως σε χρήστες υπολογιστών χωρίς ιδιαίτερη εμπειρία. Έτσι, αποφύγαμε κατά το δυνατόν τεχνικές λεπτομέρειες και δυσνόητους όρους, ενώ αντλήσαμε τα παραδείγματα από απλές καθημερινές καταστάσεις.

Ελπίζουμε οτι θα τον βρείτε ευανάγνωστο και κατανοητό, οτι θα χρησιμεύσει στην εργασία σας και οτι, σταδιακά, θα την απλουστεύσει. Πάνω από όλα όμως, ελπίζουμε οτι θα σας βοηθήσει να διακρίνετε, να αποφεύγετε και, κατά περίπτωση, να αντιμετωπίζετε τους πιο συνηθισμένους ψηφιακούς κινδύνους, βελτιώνοντας την ασφάλεια τόσο σε εργασιακό όσο και σε προσωπικό επίπεδο. Ας μην ξεχνάμε οτι, στο άμεσο μέλλον, όλες μας οι συσκευές θα λειτουργούν στο (ή με το) διαδίκτυο - το “διαδίκτυο των αντικειμένων” (Internet Of Things) είναι πλέον η νέα πραγματικότητα.

Για το τυπικό: **ο συγγραφέας του εγχειριδίου αυτού και οποιοσδήποτε άλλος τυχόν συνέβαλε σε αυτό, περιλαμβανομένου του Δήμου Μεγαρέων αλλά όχι μόνο, δεν φέρουν καμμία απολύτως ευθύνη για οποιαδήποτε ζημιά, από ή προς οποιονδήποτε, που προέκυψε από την εφαρμογή ή τη μή εφαρμογή ή την κακή εφαρμογή των όσων αναφέρονται σε αυτό. Με άλλα λόγια, διαβάζετε ή/και εφαρμόζετε τα όσα γράφονται εδώ, αποκλειστικά με δική σας ευθύνη.**

ΙΙ. Η έννοια της ασφάλειας

Η λέξη «ασφάλεια» μπορεί να αναφέρεται σε σχεδόν οτιδήποτε. Από μια ασφάλεια ζωής μέχρι την ασφάλεια του ηλεκτρικού πίνακα και από μια πόρτα ασφαλείας μέχρι την ασφάλεια των τραπεζικών συναλλαγών ή την ασφάλεια των δεδομένων. Αυτή η τελευταία περίπτωση είναι που θα μας απασχολήσει, στο βαθμό που σχετίζεται με την εργασία μας σε υπολογιστή, την καθημερινότητά μας στο Δήμο δηλαδή. Σε κάποιες περιπτώσεις θα επεκταθούμε λίγο παραπάνω, για να καλύψουμε συνηθισμένες καταστάσεις και πρακτικές, έστω κι αν δεν εμπίπτουν αυστηρά στο πλαίσιο της εργασίας μας.

Η ασφάλεια ενός συστήματος (πράγμα, κατάσταση, ενέργεια, επιχείρηση) είναι σαν μια αλυσίδα, που κάθε κρίκος της προστατεύει από ένα κίνδυνο. Όπως η αλυσίδα, έτσι και η ασφάλεια, εάν η δύναμη που την τεντώνει (η απειλή) ξεπεράσει κάποια όρια, θα σπάσει στον πιο αδύναμο κρίκο: η υπόλοιπη θα είναι άθικτη αλλά άχρηστη.
Συμπέρασμα: δεν έχει καμία απολύτως αξία να έχουμε ορισμένα στοιχεία τέλεια ασφαλισμένα, όταν υπάρχουν στοιχεία στα οποία δεν έχουμε δώσει προσοχή. Ασφάλεια σημαίνει πάνω απ' όλα ισορροπία: όλοι οι πιθανοί κίνδυνοι να έχουν προβλεφθεί, όλοι οι «κρίκοι» να έχουν ελεγχθεί.

Ας δούμε πιο πρακτικά την έννοια της ασφάλειας, μέσα από μερικές καταστάσεις που, μέσες άκρες, όλοι γνωρίζουμε:

Στην ασφάλεια εντός κτιρίου παίζει σημαντικό ρόλο το σίδερο στα δοκάρια.
Αν βάλουμε διπλάσιο σίδερο σίγουρα έχουμε μεγαλύτερη ασφάλεια. Αν όμως μείνουν κενά (αέρας) στα σημεία που το τσιμέντο ακουμπάει στο σίδερο, δεν υπάρχει ασφάλεια: στον παραμικρό σεισμό θα σπάσουν οι κολώνες, όσο σίδερο κι αν έχουμε βάλει. Οπότε, δεν προσφέρει τίποτα το σίδερο αν μια ελάχιστη κακοτεχνία αποδειχθεί "αδύναμος κρίκος" (στην περίπτωσή μας, οι φυσαλίδες αέρα).
Συμπέρασμα: προβλέπουμε και φροντίζουμε για όλες τις απειλές εξίσου.

Σε ένα κτίριο γραφείων κάποιος φωνάζει δυνατά "φωτιά".
Ο περισσότερος κόσμος, πανικόβλητος, τρέχει προς το πιο προφανές σημείο (στις σκάλες ή σε κάποια έξοδο) για να ξεφύγει, χωρίς να έχει δει φωτιά ή καπνό. Ελάχιστοι έχουν την ψυχραιμία να δουν εάν και πού υπάρχει φωτιά, να εξετάσουν τρόπους διαφυγής ή προστασίας, να ζητήσουν βοήθεια κλπ. Στην πραγματικότητα, ο κίνδυνος να υπάρξουν τραυματισμοί ή θάνατοι από τις αντιδράσεις πανικού είναι συχνά μεγαλύτερος από την ίδια τη φωτιά.
Συμπέρασμα: πρώτα εκτιμάμε ψύχραιμα τον κίνδυνο και μετά ενεργούμε.

Πώς εκτιμάμε τον κίνδυνο; Ας δούμε ένα επίκαιρο παράδειγμα.
Στα εμβόλια, γίνεται εκτίμηση κινδύνου, όπως σε πολλά πράγματα (φάρμακα, παιχνίδια, γέφυρες, επιχειρηματικές και πολιτικές αποφάσεις κλπ) που, εντελώς απλοϊκά, πάει κάπως έτσι:
- Πόσοι το έκαναν; 1000. - Πόσοι πέθαναν; 3. - Πόσοι έζησαν; 997.
- Πόσοι νόσησαν; 900. - Πόσοι νοσηλεύτηκαν; 100
Μια εκτίμηση κινδύνου λέει οτι το εμβόλιο είναι σημαντικός παράγοντας ασφαλείας, αφού προστατεύει σε ποσοστό 90% με κίνδυνο θανάτου 3 στα 1000.

Εκτίμηση κινδύνου σε υπολογιστικά συστήματα

Στους παρακάτω πίνακες θα δείτε δυο ρεαλιστικά παραδείγματα εκτίμησης κινδύνου για πληροφοριακά συστήματα. Αφορούν σε ένα κτίριο γραφείων παρόμοιο με το κτίριο του Δήμου, όπου εργάζονται αρκετά άτομα σε υπολογιστή (workstations), ενώ φιλοξενούνται και λίγοι εξυπηρέτες (servers). Είναι δυο διαφορετικοί, αλλά εξίσου αξιόλογοι, τρόποι παρουσίασης μιας μελέτης εκτίμησης κινδύνων.

ΑΠΕΙΛΗ	ΑΔΥΝΑΜΙΑ	ΑΦΟΡΑ	ΕΠΙΠΤΩΣΗ	ΠΙΘΑΝΟΤΗΤΑ	ΕΚΤΙΜΗΣΗ Κ.	ΣΥΣΤΑΣΗ
Υπερθέρμανση στο δωμάτιο των servers. ΜΕΓΑΛΟ	Το κλιματιστικό είναι 10-15 ετών. ΜΕΓΑΛΟ	Τους servers. ΚΡΙΣΙΜΟ	Όλες οι υπηρεσίες (λογιστήριο, μισθοδοσία) θα διακοπούν για 3+ ώρες. ΚΡΙΣΙΜΟ	Η θερμοκρασία του δωματίου αυτή τη στιγμή είναι 40 βαθμοί. ΜΕΓΑΛΟ	Πιθανή απώλεια 20.000 ευρώ ανά συμβάν. ΜΕΓΑΛΟ	Αλλαγή κλιματιστικού με κόστος 600 ευρώ.
Φυσική καταστροφή: πλημμύρα ΜΕΓΑΛΟ	Οι servers είναι στο υπόγειο. ΜΕΓΑΛΟ	Τους servers. ΚΡΙΣΙΜΟ	Θα διακοπούν όλες οι υπηρεσίες για άγνωστο διάστημα. ΚΡΙΣΙΜΟ	Η τελευταία πλημμύρα έγινε πριν 10 χρόνια. ΜΙΚΡΟ	Απίθανο να συμβεί, μετά και τις αντλίες που μπήκαν. ΜΙΚΡΟ	Τακτικός έλεγχος των αντλιών και αποχετεύσεων.
Ανθρώπινο λάθος – διαγραφή αρχείων. ΜΕΓΑΛΟ	Το λογισμικό δεν ελέγχεται συστηματικά. Τα backup είναι καθημερινά. ΚΡΙΣΙΜΟ	Όλους τους υπολογιστές του προσωπικού (workstations). ΜΕΤΡΙΟ	Κρίσιμα στοιχεία μπορεί να χαθούν αλλά και να ανακτηθούν από το backup. ΜΙΚΡΟ	Το προσωπικό δεν έχει ιδιαίτερη εκπαίδευση σε υπολογιστές. ΜΕΓΑΛΟ	ΜΕΤΡΙΟ – ΒΑΙΝΕΙ ΜΕΙΟΥΜΕΝΟ	Εκπαίδευση του προσωπικού για ασφαλή χρήση η/υ.
Συστεμική επίθεση DDOS στο server του λογιστηρίου. ΜΕΓΑΛΟ	Υπάρχει τείχος προστασίας και έχει ρυθμιστεί για DDOS. ΜΙΚΡΟ	Λογιστήριο, Μισθοδοσία ΚΡΙΣΙΜΟ	Απώλεια ή χάλκευση δεδομένων, διακοπή λειτουργίας κλπ. ΚΡΙΣΙΜΟ	Τελευταία φορά ήταν πριν 2 χρόνια και διήρκεσε 3 λεπτά. ΜΕΤΡΙΟ	Πιθανή απώλεια 30.000 ευρώ ανά συμβάν. ΜΕΤΡΙΟ	Τακτικός έλεγχος και αναβάθμιση τείχους προστασίας.

ΑΔΥΝΑΜΙΑ	ΚΙΝΔΥΝΟΙ	ΠΙΘΑΝΕΣ ΑΠΩΛΕΙΕΣ	ΕΚΤΙΜΗΣΗ
Δεν ενημερώνονται τακτικά διάφορα προγράμματα στους σταθμούς εργασίας.	Ηλεκτρονικό έγκλημα Υποκλοπή στοιχείων Απώλεια ελέγχου η/υ	Εμπιστευτικότητα και εγκυρότητα εγγράφων και πληροφοριών	Υψηλός κίνδυνος. Πρέπει να γίνονται αυτόματα όλες οι ενημερώσεις λογισμικού και να ελέγχονται τακτικά.
Έχουν πρόσβαση στο server μή εξουσιοδοτημένα ή/και μή εκπαιδευμένα άτομα.	Ηλεκτρονικό έγκλημα Υποκλοπή και χάλκευση στοιχείων Διαρροή προσωπικών δεδομένων	Εμπιστευτικότητα και αξιοπιστία του συνόλου των πληροφοριών, μεταξύ αυτών και ευαίσθητων-προσωπικών δεδομένων.	Υψηλός κίνδυνος. Η πρόσβαση στο server πρέπει να καθορίζεται ρητά και να ελέγχεται αυστηρά.
Λειτουργικά συστήματα και υπολογιστές 10+ ετών.	Απώλεια και χάλκευση δεδομένων Κερκόπορτα για εισβολείς	Αξιοπιστία δεδομένων, ειδικά αν δεν υπάρχουν διαδοχικά backup έως και ένα μήνα πίσω. Έλεγχος η/υ από τρίτους.	Μέτριος κίνδυνος, εφόσον τηρούνται τα backup και εφόσον υπάρχει σύστημα εντοπισμού εισβολέων. Να ενημερωθούν τα λειτουργικά.

III. Ορισμοί και Διαδικασίες

Λέγοντας “προσωπικά δεδομένα” εννοούμε κάθε λογής πληροφορίες που αφορούν ταυτοποιημένα ή ταυτοποιήσιμα φυσικά πρόσωπα. Με απλά λόγια, όλες οι πληροφορίες που μπορεί να οδηγήσουν στον εντοπισμό ενός προσώπου, από το όνομα και τον αριθμό της ταυτότητάς του μέχρι τον τραπεζικό του λογαριασμό και το πού βρίσκεται ή τί ακριβώς κάνει μια συγκεκριμένη χρονική στιγμή. Επιπλέον, λέγοντας “ευαίσθητα προσωπικά δεδομένα” εννοούμε τις πληροφορίες εκείνες που μπορεί να αποκαλύψουν τη φυλετική ή εθνοτική καταγωγή ενός προσώπου, τα πολιτικά του φρονήματα, τις θρησκευτικές του πεποιθήσεις, όπως και στοιχεία γενετικά ή βιολογικά, υγείας, σεξουαλικής ζωής κλπ. Αυτές οι προσωπικές πληροφορίες απαιτούν ειδικό χειρισμό, σύμφωνα με το νόμο (GDPR: Κανονισμός Προστασίας Προσωπικών Δεδομένων).

Σε αυτό τον Οδηγό, για ευκολία, εξετάζουμε ενιαία όλες αυτές τις πληροφορίες που απαιτούν ασφάλεια, έστω κι αν δεν πρόκειται κυριολεκτικά ή αποκλειστικά για προσωπικά δεδομένα.
Θα δούμε στη συνέχεια τα βήματα που βελτιώνουν την ασφάλεια τέτοιων πληροφοριών.

1. Καταγραφή και αξιολόγηση

Οι ερωτήσεις που πρέπει να απαντήσουμε είναι:
- Ποιες εμπιστευτικές πληροφορίες έχουμε ή/και διαχειριζόμαστε στον υπολογιστή μας;
Ενδεικτικά: emails ή/και τηλέφωνα ή/και διευθύνσεις κατοικίας ή/και αιτήματα πολιτών και υπαλλήλων, στοιχεία μισθοδοσίας, τραπεζικούς λογαριασμούς, πληροφορίες υγείας ή ασφάλισης, προσωπικούς κωδικούς (passwords), φορολογικά στοιχεία…
- Πώς διαχειριζόμαστε και προστατεύουμε αυτές τις πληροφορίες;
Ενδεικτικά: κρατάμε τακτικά αντίγραφα ασφαλείας, δεν στέλνουμε emails με πολλαπλούς παραλήπτες χωρίς ιδιαίτερο λόγο και ειδικά όταν δεν πρέπει να αναγνωρίζει ο ένας παραλήπτης τον άλλο (χρησιμοποιούμε Κρυφή Κοινοποίηση όπου χρειάζεται), τηρούμε το Δεκάλογο Ασφάλειας, διαβάζουμε και τηρούμε τις συστάσεις των Αρχών για τυχόν νέες απειλές…
- Ποιος έχει πρόσβαση στις ελεγχόμενες πληροφορίες και υπό ποιες προϋποθέσεις;
Ενδεικτικά: πρόσβαση στη μισθοδοσία ή στα ιατρικά δεδομένα ή στα στοιχεία του προσωπικού πρέπει να έχουν μόνο εργαζόμενοι στο σχετικό τμήμα και με ευθύνη τους να τα προστατεύουν από μή εξουσιοδοτημένα άτομα (είτε από το προσωπικό του Δήμου είτε όχι).

2. Διασφάλιση

Αφού καταγραφούν οι “ευαίσθητες” πληροφορίες, όσες δηλαδή χρειάζονται προστασία, φροντίζουμε κατ’ αρχήν να τις αποθηκεύουμε σε ασφαλή χώρο. Ενδεικτικά, ένα USB stick δεν παρέχει ιδιαίτερη ασφάλεια (μπορεί να χαθεί, να κλαπεί, να χαλάσει) ενώ ένας server κλειδωμένος σε κάποιο υπόγειο και χωρίς σύνδεση στο internet, είναι ικανοποιητικά ασφαλής.

3. Τυποποίηση

Κάθε Διεύθυνση ή/και Τμήμα οφείλει να έχει έναν Κανονισμό για την ασφάλεια των πληροφοριών που διαχειρίζεται, εστιάζοντας και εξειδικεύοντας σε όσες απαιτούν ειδικό χειρισμό. Ο Κανονισμός αυτός καταγράφει τις ενέργειες και διαδικασίες που πρέπει να ακολουθεί οποιοσδήποτε έρχεται σε επαφή με αυτές τις πληροφορίες, κατά τρόπο που από τη μία να μην υπάρχει αμφιβολία στο ερώτημα “τί κάνω τώρα” και από την άλλη να προλαμβάνονται τυχόν

λανθασμένες ή αντικρουόμενες ενέργειες. Σε γενικές γραμμές πρέπει να προβλέπονται, ανάλογα το Τμήμα, οδηγίες χειρισμού για τα παρακάτω τουλάχιστον:

- Στοιχεία και πληροφορίες Δημοτών
- Προσωπικές πληροφορίες υπαλλήλων και αιρετών
- Κάθε πληροφορία που μπορεί να οδηγήσει σε ταυτοποίηση προσώπου (ονοματεπώνυμο, ΑΦΜ, διεύθυνση κατοικίας ή email, τηλέφωνο, ηλικία, τόπος γέννησης κλπ), καθώς και όλα τα "ευαίσθητα προσωπικά δεδομένα", όπως ορίστηκαν νωρίτερα.
- Κάθε πληροφορία που έχει χαρακτηριστεί σαν "ειδικού χειρισμού" (απόρρητη, εμπιστευτική κλπ).

4. "Ευαίσθητες" πληροφορίες από το internet

Στο διαδίκτυο λειτουργούν αρκετές ιστοσελίδες του Δήμου ή συνεργαζόμενες με το Δήμο, με τις οποίες αλληλεπιδρούμε και από τις οποίες αντλούμε πληροφορίες, όπως οι διάφορες εφαρμογές του intelligent city ή οι δηλώσεις τετραγωνικών ακινήτων. Παρότι κάποιες φορές το παραβλέπουμε, οι πληροφορίες που αντλούμε από εκεί χρήζουν επίσης προστασίας, τόσο κατά τη συλλογή τους όσο και, τοπικά, κατά την επεξεργασία τους. Πρέπει να δηλαδή να ελέγχουμε και να εγγυώμαστε για την ασφάλειά τους τόσο ως προς τον πάροχο της υπηρεσίας που τις συλλέγει ή/και καταχωρεί, όσο και στους υπολογιστές του Δήμου στους οποίους γίνεται αποθήκευση και επεξεργασία.

5. Ασφάλεια πολλών επιπέδων

Σε κάθε κατάσταση στην οποία απαιτείται ασφάλεια, δημιουργούμε πολλά επίπεδα προστασίας και ελέγχου, ανάλογα την εκάστοτε ανάγκη.

Για παράδειγμα, σε ένα σπίτι βάζουμε κλειδαριά στην αυλόπορτα αλλά και στην πόρτα εισόδου ενώ, αν έχουμε κάτι πολύτιμο, ίσως το φυλάσσουμε σε ένα χρηματοκιβώτιο. Για να κινδυνεύσει το πολύτιμο περιεχόμενο του χρηματοκιβωτίου, πρέπει ο εισβολέας να παραβιάσει τρία επίπεδα προστασίας στη σειρά (τις τρεις κλειδαριές), τουλάχιστον. Αν παραβιάσει μόνο το πρώτο επίπεδο (την κλειδαριά της αυλόπορτας) το πολύ να αποσπάσει κάποιο ευτελές αντικείμενο που φυλάσσουμε στην αυλή ή στον κήπο.

Με το ίδιο σκεπτικό και την ίδια διαδικασία ασφαλίζουμε τα δεδομένα μας στον ψηφιακό κόσμο: όσο πιο πολύτιμα τα δεδομένα, τόσο περισσότερα τα επίπεδα προστασίας. Για παράδειγμα, ένας δύσκολος κωδικός (password) εισόδου στον υπολογιστή μας, προσφέρει μια καλή ασφάλεια πρώτου επιπέδου. Αν όμως στον υπολογιστή μας αποθηκεύουμε ευαίσθητα προσωπικά δεδομένα, τότε αυτά απαιτούν επιπλέον προστασία, για τον ίδιο λόγο που δεν αφήνουμε τα κοσμήματά μας στην αυλή ή στον κήπο: δεν μας αρκεί μία μόνο "κλειδαριά" αφού, αν αυτή παραβιαστεί, δε θα υπάρχει τίποτα να τα προστατεύσει.

Θυμόμαστε: η ασφάλεια δεδομένων υλοποιείται με πολλά επίπεδα ελέγχου και προστασίας.

Επίπεδα ελέγχου-προστασίας

Τα επίπεδα αυτά υλοποιούνται ή εφαρμόζονται τόσο τεχνικά όσο και με διοικητικές διαδικασίες.

Σε κάθε περίπτωση, ξεκινάμε από την καταγραφή όλων των πληροφοριών που επεξεργαζόμαστε και αποθηκεύουμε στον υπολογιστή μας ή αλλού. **Είναι πολύ σημαντικό να καταγραφούν όλοι οι τύποι πληροφοριών και ο τελικός κατάλογος να είναι πλήρης**, ώστε από τη μία να είμαστε βέβαιοι οτι δεν έχει διαφύγει κάτι κρίσιμο και από την άλλη να μπορούμε να εντοπίσουμε και εκτιμήσουμε με ακρίβεια τη ζημιά, σε περίπτωση απώλειας, κλοπής, αλλοίωσης κλπ.

Χαρακτηρισμός δεδομένων

Η ταξινόμηση των ψηφιακών δεδομένων ως προς το βαθμό ασφάλειας που απαιτούν, όπως ακριβώς η διαβάθμιση των εγγράφων, καθορίζει τον κατάλληλο τρόπο χειρισμού τους. Μπορεί κάποιος να ορίσει διάφορες "ετικέτες" χειρισμού, ανάλογα το αντικείμενο και την ανάγκη. Μερικές συνηθισμένες είναι: **Αυστηρά Προσωπικό – Απόρρητο – Εμπιστευτικό - Για εσωτερική χρήση - Προσωπικά Δεδομένα – Αδιαβάθμιστο** (άνευ).

Έλεγχος πρόσβασης

Ο γενικός κανόνας είναι "όσο πιο σημαντικές ή ευαίσθητες οι πληροφορίες, τόσο περισσότεροι και αυστηρότεροι οι έλεγχοι πρόσβασης". Από τη στιγμή που γνωρίζουμε τις κατηγορίες των πληροφοριών που χειριζόμαστε και τις έχουμε διαβαθμίσει ως προς την ασφάλεια που απαιτούν, καθορίζουμε τους απαιτούμενους ελέγχους πρόσβασης: εκχωρούμε δικαιώματα πρόσβασης σε συγκεκριμένα άτομα. Παράδειγμα τέτοιων δικαιωμάτων είναι: **κανένα - μόνο ανάγνωση – διόρθωση – διαγραφή**. Στην πράξη, φτιάχνουμε μια κατάσταση με τα άτομα που χρειάζονται πρόσβαση σε κάθε κατηγορία πληροφοριών, καθώς και τις υποχρεώσεις εχεμύθειας και προστασίας που αναλαμβάνουν. Η κατάσταση πρέπει να περιλαμβάνει: πληροφορία - άτομο – δικαιώματα – προϋποθέσεις και υποχρεώσεις.

Διασφάλιση με τεχνικά μέσα

Λέγοντας τεχνικά μέσα, εννοούμε κυρίως τους κωδικούς πρόσβασης (passwords) και την κρυπτογράφηση. Η κρυπτογράφηση των αρχείων ή της μετάδοσης πληροφοριών γίνεται από κατάλληλο λογισμικό, την εγκατάσταση του οποίου αναλαμβάνει ειδικευμένος τεχνικός, όπως και την τυχόν εκπαίδευση σε αυτό, εφόσον χρειάζεται. Για τους κωδικούς πρόσβασης πιθανότατα γνωρίζετε ήδη πόσο σημαντικοί είναι και πώς να τους ορίζετε.
Σε συντομία, ένας κωδικός για να είναι σχετικά ασφαλής πρέπει να:
- έχει μήκος τουλάχιστον 10 χαρακτήρων
- περιέχει γράμματα, αριθμούς και σύμβολα
- μην συμπίπτει με ήδη γνωστές πληροφορίες του ατόμου
- μην χρησιμοποιείται σε πολλές εφαρμογές

Αντίγραφα ασφαλείας

Εάν υπήρχε μία μόνο μέθοδος διασφάλισης των ψηφιακών δεδομένων, αυτή θα ήταν τα αντίγραφα ασφαλείας (backups). Τα αρχεία και οι πληροφορίες μπορεί να χαλκευτούν, να κλαπούν, να χαθούν και γενικά να καταστραφούν με πολλούς τρόπους αλλά, οι μισοί και πλέον κίνδυνοι μπορούν να αποσοβηθούν ή ελαχιστοποιηθούν αν υπάρχει αντίγραφο ασφαλείας. Ο Δήμος έχει μια γενική διαδικασία, αλλά κάθε Τμήμα ή Διεύθυνση χρειάζεται ένα Κανονισμό εξειδικευμένο ως προς το αντικείμενο και τις ανάγκες. Μεταξύ άλλων, στον Κανονισμό αυτό πρέπει να ορίζονται: ο τρόπος και η συχνότητα λήψης αντιγράφων, η διάρκεια διατήρησής τους, τα άτομα που ελέγχουν την εφαρμογή του κανονισμού, τη διαδικασία επαναφοράς σε περίπτωση ανάγκης, το χώρο που φυλάσσονται τα τυχόν φορητά μέσα (πχ usb stick), τα άτομα που έχουν πρόσβαση εκεί κλπ...

6. Σε περίπτωση παραβίασης

Όσο καλή κι αν είναι η ασφάλεια, σε οποιοδήποτε περιβάλλον, πάντα υπάρχει η πιθανότητα ατυχήματος ή παραβίασης που, πέρα από άλλης μορφής ζημιά, μπορεί να έχει διοικητικές και νομικές συνέπειες. Εάν συμβεί, εξειδικευμένοι τεχνικοί θα φροντίσουν να περιορίσουν ή διορθώσουν τη ζημιά και να βελτιώσουν το πρόγραμμα ή τη διαδικασία που το προκάλεσε. Για

όλους τους μή ειδικούς, ο γενικός κανόνας είναι ένας: **εάν αντιληφθούμε οποιοδήποτε πρόβλημα ή δυσλειτουργία, καλούμε αμέσως την υποστήριξη** – δεν παίρνουμε καμία πρωτοβουλία αν δεν έχουμε τις γνώσεις και την εξουσιοδότηση. Η μόνη εξαίρεση είναι να ακολουθήσουμε τις οδηγίες στο **Σχέδιο Αντιμετώπισης Έκτακτης Ανάγκης**, εφόσον υπάρχει και καλύπτει την περίπτωσή μας.

IV. Πρακτικά Παραδείγματα

Μέχρι τώρα είδαμε το ζήτημα της ασφάλειας κάπως θεωρητικά: τους ορισμούς, τις διαδικασίες και κάποιες γενικές οδηγίες και υποχρεώσεις. Αφήνοντας προς το παρόν τις περιπτώσεις ατυχήματος, θα εξετάσουμε τις πιο συνηθισμένες απειλές στην πράξη και κυρίως τις ψηφιακές απάτες.

1. Κοινωνική μηχανική

Πιο γνωστή με τον αγγλικό της όρο (social engineering), η κοινωνική μηχανική είναι μια απάτη κατά την οποία ένα άτομο παραπλανάται ή/και χειραγωγείται ώστε να αποκαλύψει εμπιστευτικές πληροφορίες, οι οποίες χρησιμοποιούνται για την παράκαμψη κάποιας ασφάλειας. Είναι μια αποτελεσματική μέθοδος εξαπάτησης επειδή ο έμπειρος απατεώνας κάνει ό,τι μπορεί ώστε οι ενέργειές του να δείχνουν νόμιμες, χρήσιμες, έως και φιλικές, ώστε εύκολα μπορεί να παραπλανηθεί ο καθένας.

Η κοινωνική μηχανική εφαρμόζεται τόσο online όσο και στην πραγματική ζωή. Στην εικόνα βλέπουμε επιγραμματικά τα στάδια (και το σχέδιο δράσης):

Θα έχετε ακούσει την κλασσική πλέον απάτη που κάποιος απελπισμένος, με αναφιλητά, μας καλεί και μας ανακοινώνει οτι ένας στενός συγγενής μας έχει πέσει θύμα ατυχήματος και έχει κατεπείγουσα ανάγκη από χρήματα για να χειρουργηθεί. Αυτή επαναλαμβάνεται και στον ψηφιακό κόσμο, με διάφορες παραλλαγές όπως όταν εμφανίζονται πολλά αναδυόμενα παράθυρα (pop-ups) με προειδοποιήσεις περί κινδύνων ή ασυνήθιστες “ανακοινώσεις” που ζητάνε προσωπικές πληροφορίες ή/και μικροποσά δήθεν για βελτίωση της ασφάλειας. Προσοχή χρειάζεται και όταν δήθεν “βρίσκουμε” ένα USB stick (το δόλωμα), το οποίο μπορεί να περιέχει κακόβουλο λογισμικό. Ένα σημαντικό σημείο προσοχής είναι οτι τα κοινωνικά δίκτυα, όπως το Facebook, προσφέρουν άφθονο “υλικό” οπότε, αν κάποιος κακόβουλος θελήσει να παραστήσει ένα φίλο ή συγγενή μας, σίγουρα γνωρίζει αρκετά προσωπικά στοιχεία για να μας παγιδεύσει.

Με αυτά, καταλαβαίνουμε οτι δεν χρειάζεται ιδιαίτερο ταλέντο για τέτοια απάτη που δυστυχώς μπορεί να πάρει πολλές μορφές, πέραν αυτής του παραδείγματος.

Ο μόνος τρόπος προστασίας είναι η εκπαίδευση: μαθαίνουμε να διακρίνουμε τα σημεία εκείνα που μαρτυρούν απάτη.

Στην εικόνα βλέπουμε τα πλέον βασικά.

2. Πλαστοπροσωπία (fraud)

Η απάτη της πλαστοπροσωπίας (αλλά και της αντιποίησης αρχής), όταν δηλαδή ένας επίδοξος εισβολέας υποκρίνεται οτι είναι κάποιος άλλος, συνήθως περιλαμβάνεται στον όρο “fraud”. Σαν γενική αρχή, δεν ζητάμε ποτέ εμπιστευτικές και προσωπικές πληροφορίες από τρίτους, ειδικά αν δεν είμαστε απολύτως βέβαιοι για την κατάλληλη διαχείρισή τους (έλεγχος αποστολέα, διασταύρωση περιεχομένου, ασφαλής μετάδοση και αποθήκευση κλπ), ενώ ταυτόχρονα ενημερώνουμε τα άτομα με τα οποία έχουμε επικοινωνία οτι ποτέ δε θα ζητήσουμε προσωπικές τους πληροφορίες και ιδίως μέσω Facebook ή με τρόπο μή εγκεκριμένο για τη δουλειά αυτή. Ένας λόγος που δε ζητάμε προσωπικές πληροφορίες χωρίς κατάλληλες εγγυήσεις είναι οτι, αν εμείς λειτουργούμε “απρόσεκτα”, είναι πολύ εύκολο για κάποιον κακόβουλο να μας υποδυθεί. Στο ίδιο πλαίσιο είναι και ο λεπτομερής έλεγχος του αποστολέα, που πρέπει να μας γίνει συνήθεια. Ενδεικτικά: έχει άραγε ο Δήμαρχος διεύθυνση dmegaara@megara.gr ; (όχι, το email έχει ένα a παραπάνω, επομένως είναι κάποιος που τον υποκρίνεται)

3. Ψάρεμα (phishing)

Σε αυτή την τεχνική ο εισβολέας παραπλανά το υποψήφιο θύμα ώστε να νομίζει οτι έχει να κάνει με κάποια γνωστή και έμπιστη ιστοσελίδα ή υπηρεσία κλπ. Για παράδειγμα, στην περίπτωση του Δήμου, μπορεί κάποιος κακόβουλος να φτιάξει μια ιστοσελίδα με όνομα “megarra.gr” (προσέξτε οτι έχει δύο “r”) και να αντιγράψει σε αυτήν, πλήρως, την εμφάνιση και το περιεχόμενο της πραγματικής (megara.gr). Το μόνο που του μένει είναι, με κάποιο τρόπο, να προσκαλέσει υπαλλήλους ή και Δημότες να “συνδεθούν” σε κάποια από τις παρεχόμενες υπηρεσίες του δήθεν Δήμου: όλα τα στοιχεία που θα εισάγουν τα ανυποψίαστα θύματα, θα περάσουν στην κατοχή του. Στην ίδια τεχνική ανήκουν και τα e-mails που μοιάζουν γνήσια και από έμπιστο αποστολέα (συνήθως κάποια τράπεζα) και ζητούν να κατεβάσετε κάποιο αρχείο ή να πατήσετε κάποιο σύνδεσμο. Οι απατεώνες αυτής της τεχνικής συχνά εκμεταλλεύονται τη σύγχυση ή το μικροπανικό που προκαλείται από κάποια φωτιά ή πλημμύρα, την πανδημία, κάποια οικονομική είδηση, τις διακοπές, ακόμα και τις εκλογές: είναι οι περίοδοι που τέτοιες τεχνικές “ανθούν”.

Και σε αυτή την περίπτωση, **η μόνη προστασία είναι η εκπαίδευση**: πρέπει όλοι να γνωρίζουμε αν και πότε, με email ή τηλέφωνο ή άλλο μέσον, κάποιος μας “ψαρεύει”.

Ενδεικτικά:

- δε ζητάμε προσωπικά στοιχεία χωρίς εγκεκριμένη μέθοδο-διαδικασία
- δηλώνουμε παντού οτι κανείς από το Δήμο δε θα ζητήσει κωδικούς ή απόρρητα στοιχεία
- δεν πατάμε συνδέσμους σε emails αν δεν είμαστε απολύτως βέβαιοι οτι είναι γνήσιοι
- σε περίπτωση αμφιβολίας γράφουμε τη διεύθυνση με το χέρι (διεύθυνση επίσκεψης στο browser, διεύθυνση e-mail του παραλήπτη κλπ)
- όταν μας καλούν (με τηλέφωνο ή e-mail) και ζητούν προσωπικά μας στοιχεία δεν τα δίνουμε εφόσον δεν μπορούμε να επαληθεύσουμε αξιόπιστα τον καλούντα (αποστολέα) – αντιθέτως, τον καλούμε εμείς σε διεύθυνση ή αριθμό που γνωρίζουμε οτι είναι αληθινός (όχι σε διεύθυνση ή αριθμό που ίσως μας δώσει)
- εάν υποψιαζόμαστε οτι πέσαμε θύματα ψαρέματος, ειδοποιούμε αμέσως τη σχετική υπηρεσία (τεχνική υποστήριξη, τράπεζα κλπ) και αλλάζουμε τους κωδικούς που τυχόν διέρρευσαν

4. Απατηλή προστασία

Μια από τις πιο δημοφιλείς και επιτυχημένες απάτες στηρίζεται στην προώθηση προγραμμάτων που δήθεν προστατεύουν ή καθαρίζουν τον υπολογιστή από μικρόβια και άλλα προβλήματα, ενώ στην πραγματικότητα πρόκειται για κακόβουλο λογισμικό που μπορεί να λειτουργεί σαν μικρόβιο, να υποκλέπτει τις επικοινωνίες μας, να χαλκεύει τα αρχεία μας κλπ. Είναι ένας ακόμη λόγος που ποτέ δεν εγκαθιστούμε προγράμματα στον υπολογιστή μας, αν δεν είμαστε απολύτως βέβαιοι για την αυθεντικότητα και την ασφάλειά τους.
Σε κάθε περίπτωση, **εάν εμφανιστεί ειδοποίηση** προβλήματος στον υπολογιστή (μικρόβιο ή άλλο) ή οποιοδήποτε ασυνήθιστο μήνυμα, **καλούμε αμέσως την τεχνική υποστήριξη, χωρίς να προβούμε σε καμία άλλη ενέργεια**.

5. Κακόβουλο λογισμικό

Επικίνδυνα (κακόβουλα) προγράμματα μπορεί να βρεθούν οπουδήποτε στο διαδίκτυο: όταν κατεβάζουμε “κάτι από κάπου”, σαν συνημμένα αρχεία σε κάποιο email, μέσω κοινωνικών δικτύων κλπ. Ιδιαίτερα επικίνδυνα είναι αυτά που αντιγράφουν κάθε μας πληκτρολόγηση (κωδικούς, κείμενα, chat, αριθμούς καρτών και οτιδήποτε άλλο γράφουμε με το πληκτρολόγιο), στέλνοντας αυτές τις κρίσιμες πληροφορίες σε έναν απατεώνα με καταστροφικό, συνήθως, αποτέλεσμα.
Μπορούμε να αποφύγουμε σχεδόν εντελώς τέτοιας μορφής λογισμικό, αν ενημερώνουμε τακτικά τα κανονικά μας προγράμματα, το όποιο πρόγραμμα προστασίας (πχ Avast) καθώς και το λειτουργικό σύστημα (πχ Windows).

6. Adware – Spyware

Προγράμματα που λειτουργούν αφανώς (στο παρασκήνιο) και επηρρεάζουν την κανονική λειτουργία του υπολογιστή μας, ιδίως όταν παρεμβαίνουν στις εντολές μας, ανήκουν πιθανότατα σε κάποια από αυτές τις κατηγορίες λογισμικού. Λέγοντας adware εννοούμε τα προγράμματα που εμφανίζουν διαφημίσεις συνεχώς, συστηματικά και με τρόπο ενοχλητικό, με συνήθη παρενέργεια την εξαιρετικά αργή λειτουργία του υπολογιστή μας. Με τη λέξη spyware περιγράφουμε όσα προγράμματα “κατασκοπεύουν” (και πιθανότατα μεταδίδουν σε τρίτους) τις δικές μας ενέργειες – σε ορισμένες επικίνδυνες περιπτώσεις, ακόμη και την πληκτρολόγησή μας.
Για να αποφύγουμε τέτοιο λογισμικό, **δεν κατεβάζουμε προγράμματα από μή εγκεκριμένες πηγές** και **δεν εγκαθιστούμε προγράμματα των οποίων την αξιοπιστία δεν γνωρίζουμε με βεβαιότητα**.
Ενδείξεις οτι έχουμε μολυνθεί με adware ή spyware:

- ο υπολογιστής αργεί συστηματικά και αδικαιολόγητα
- εμφανίζονται υπερβολικά πολλά παράθυρα ειδοποιήσεων ή διαλόγου
- γράφουμε μια διεύθυνση στο browser και οδηγούμαστε σε άλλη

Στις περισσότερες περιπτώσεις το πρόγραμμα που ήδη έχουμε για ιούς μπορεί να "καθαρίσει" τον υπολογιστή από τέτοιο λογισμικό, με μια πλήρη σάρωση. Υπάρχουν όμως και "δύσκολες" περιπτώσεις που απαιτούν πολύ εξειδικευμένες ενέργειες. Σε κάθε περίπτωση, καλούμε την τεχνική υποστήριξη.

7. Email

Το e-mail έχει μπει για τα καλά στη ζωή μας και αυτός είναι ο λόγος που αποτελεί ένα δημοφιλές μέσον εξαπάτησης. Δείτε μια λίστα με συνηθισμένα e-mails που συγκαλύπτουν κάποιας μορφής απάτη:

7.1 Εκφοβισμός Αρχής

Σε τέτοια e-mail, κάποια κυβερνητική υπηρεσία ασφάλειας (πχ η Αστυνομία, η Αντιτρομοκρατική Υπηρεσία, η Δίωξη Ηλεκτρονικού Εγκλήματος) προσπαθεί να μας τρομάξει ώστε να δώσουμε προσωπικές ή άλλες εμπιστευτικές πληροφορίες. Ενδεικτικά παραδείγματα:
→ Απωλέσατε την ασφάλιση του ΕΦΚΑ επειδή ορισμένες πληροφορίες σας είναι ελλειπείς. Πατήστε εδώ για να τις συμπληρώσετε.
→ Κατεβάσατε παράνομα αρχεία από το Ιντερνετ. Η σύνδεσή σας θα διακοπεί μέχρι να συμπληρώσετε τα στοιχεία στην παρακάτω φόρμα.

7.2 Φιλική Προσέγγιση

Εδώ λαμβάνετε ένα μήνυμα από κάποιο γνωστό σας που σας ζητάει χρήματα για να καλύψει κάποια άμεση ανάγκη, συνήθως κάποιο ατύχημα. Σχεδόν πάντα πρόκειται για απάτη: πριν κάνετε οτιδήποτε, επικοινωνείστε τηλεφωνικά με τον αποστολέα, σαν ελάχιστη επαλήθευση.

7.3 Λάθος Παραγγελίας

Αυτή η μέθοδος είναι πολύ αποτελεσματική επειδή προσομοιάζει στην πραγματικότητα. Λαμβάνετε ένα e-mail που λέει οτι η παραγγελία σας δεν μπορεί να παραδοθεί επειδή υπάρχει κάποιο σφάλμα στα στοιχεία ή η πιστωτική σας έχει λήξει κλπ. Εάν πατήσετε στο σύνδεσμο δήθεν για να διορθώσετε το πρόβλημα, οδηγείστε σε μια πλαστή ιστοσελίδα που μοιάζει με την πραγματική αλλά σκοπό έχει να υποκλέψει τα στοιχεία που θα καταχωρίσετε.

7.4 Σύντομα Λήγει

Πρόκειται για μια πολύ δημοφιλή μέθοδο εξαπάτησης: δέχετε ένα μήνυμα που σας ενημερώνει οτι κάτι, για παράδειγμα ο λογαριασμός σας (account) στην τάδε υπηρεσία, θα λήξει σύντομα και χρειάζεται να ενημερώσετε τα στοιχεία σας. Σας δίνει κι ένα πολύ βολικό σύνδεσμο για την "ενημέρωση" που όμως οδηγεί σε πλαστή ιστοσελίδα, όμοια με την πραγματική (συνήθως μια σελίδα σύνδεσης), μέσω της οποίας ο δράστης αποκτά τα στοιχεία σας.

7.5 Εντοπισμός Παραβίασης

Εδώ, ένα καλογραμμένο μήνυμα που δείχνει "επίσημο" και μοιάζει να προέρχεται από κάποιον "σοβαρό" αποστολέα, σας ενημερώνει οτι εντοπίστηκαν παράνομες ενέργειες που οφείλονται σε πιθανή παραβίαση ενός ή περισσοτέρων λογαριασμών σας. Για να αποφύγετε περαιτέρω συνέπειες όπως η μόλυνση του υπολογιστή σας ή η απώλεια χρημάτων κλπ, καλείστε να

κατεβάσετε κάποιο συνημμένο αρχείο με οδηγίες "αποκατάστασης". Εξυπακούεται οτι, στο συνημμένο κρύβεται κάποιας μορφής παγίδα για την υποκλοπή των στοιχείων σας.

7.6 Μοναδικός Νικητής

Μια πολύ δημοφιλής μέθοδος κατά την οποία ενημερώνεστε οτι κερδίσατε ένα ποσόν ή κάποιο δώρο από πηγή που, συνήθως, δεν έχετε ξανακούσει. Καλείστε να δώσετε τα στοιχεία σας για την παραλαβή των χρημάτων ή του δώρου. Είναι πολύ καλό για να είναι αληθινό: πρόκειται για απάτη.

Δωρεά

Kendrick Anderson <homeiramasar... Σάβ 25 Δεκ 2021, 2:52 μ.μ. (πριν από 10 ημέρες)
προς κρυφή κοιν.: εγώ

Γεια σας,
Συγχαρητήρια, σας απονεμήθηκε το ποσό των τετρακοσίων χιλιάδων δολαρίων ($400.000,00 USD) Αυτό το ποσό δωρήθηκε σε εσάς από την κυρία Homeira Massoud Ardalan. Αυτή και ο σύζυγός της κέρδισαν το τζάκποτ SuperLotto Plus των ($33.000.000,00,00,00,00,00,00,00 τριών εκατομμυρίων USD) Δολάρια Ηνωμένων Πολιτειών στις 16 Μαρτίου 2013. Για περισσότερες πληροφορίες σχετικά με τον τρόπο διεκδίκησης της τιμής σας, για περισσότερες λεπτομέρειες, επικοινωνήστε μαζί της μέσω αυτού του email: homeiramasardalan@gmail.com
Ευχαριστώ.

Επικοινωνήστε μαζί της μέσω αυτού του email:homeiramasardalan@gmail.com

Απάντηση Προώθηση

7.7 Τραπεζική Ενημέρωση

Οι Τράπεζες προσφέρουν μια ευκολία, στέλνοντας ενημερωτικό e-mail όταν γίνεται ανάληψη από κάποιο λογαριασμό μας. Ο απατεώνας αντιγράφει αυτό το μήνυμα, ενημερώνοντάς μας για μια μεγάλη ανάληψη και ζητώντας επιβεβαίωση. Η σελίδα που θα οδηγηθούμε όμως είναι πλαστή, με σκοπό να υποκλέψει τις τραπεζικές πληροφορίες μας.

7.8 Θυματοποίηση

Εδώ μας κατηγορούν για κάτι πολύ σοβαρό, για το οποίο στην πραγματικότητα δεν έχουμε ιδέα. Ένας θυμωμένος πελάτης που δηλώνει οτι μας πλήρωσε και δεν στείλαμε το προϊόν, κάποιος που μετέφερε χρήματα στο λογαριασμό μας και απαιτεί να τα επιστρέψουμε, μια Τράπεζα που δήθεν μας πήρε το σπίτι κλπ. Κατά κανόνα, μας απειλούν οτι θα κάνουν αυτό κι αυτό, αν δεν επικοινωνήσουμε άμεσα μαζί τους. Όπως και προηγουμένως, υπάρχει κάποιο συνημμένο αρχείο ή ένας σύνδεσμος που στην πράξη αποτελούν μια ακόμη μέθοδο υποκλοπής των στοιχείων μας.

7.9 Εφορία

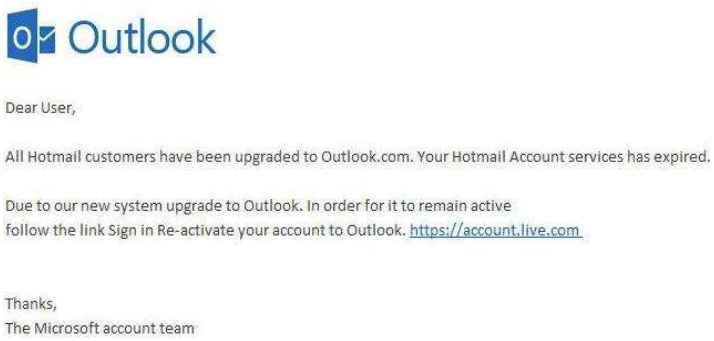
Τώρα που ψηφιοποιείται η Εφορία (ΑΑΔΕ) αρχίζει να γίνεται δημοφιλής και αυτή η μέθοδος. Μας ενημερώνει οτι έχουμε επιστροφή χρημάτων ή οτι επίκειται έλεγχος από το ΣΔΟΕ ή κάτι ανάλογο. Στο σύνδεσμο ή το συνημμένο αρχείο που περιλαμβάνεται, υπάρχει μια πλαστή σελίδα της ΑΑΔΕ στην οποία καλούμαστε να συνδεθούμε με τους κωδικούς Taxis, τους οποίους ο επίδοξος απατεώνας θα υποκλέψει.

7.10 Επαλήθευση Στοιχείων

Εδώ ενημερωνόμαστε οτι κάποια γνωστή εταιρία κάνει έλεγχο ασφαλείας και μας ζητάει να επαληθεύσουμε τα στοιχεία μας. Όπως και στα προηγούμενα, ο σύνδεσμος ή το συνημμένο επιτρέπουν την υποκλοπή των στοιχείων μας.

7.11 Αναβάθμιση Υπηρεσίας

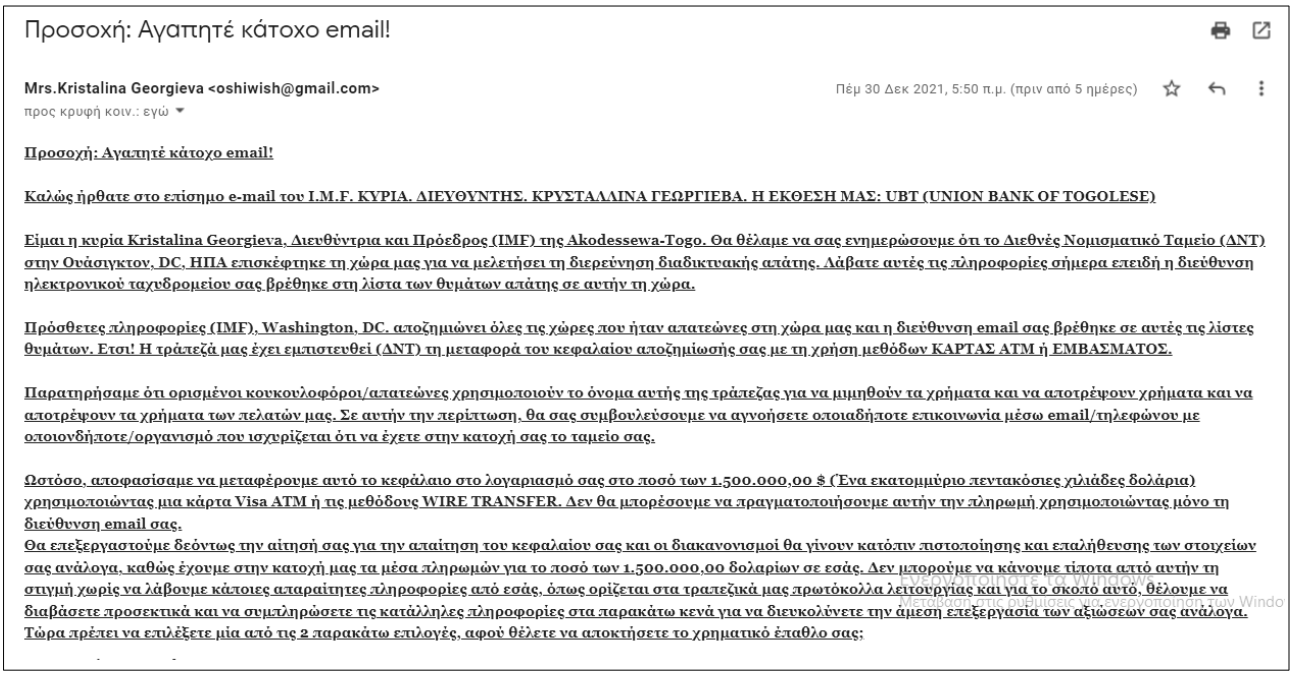
Κάποια δημοφιλής υπηρεσία (πχ Google Mail, Paypal, Outlook) μας ενημερώνει οτι ανανεώνεται και χρειάζεται να επαν-ενεργοποιήσουμε το λογαριασμό μας. Μια δύσκολα εντοπίσιμη απάτη, αφού ο σύνδεσμος που οδηγεί στην πλαστή ιστοσελίδα συχνά κρύβεται πίσω από κάποιον αληθοφανή, όπως στην εικόνα.



Τί κάνω τώρα;

Εάν λάβουμε e-mail που μοιάζει με τα παραπάνω:

- ΔΕΝ πατάμε σε συνδέσμους
- ΔΕΝ ανοίγουμε τυχόν συνημμένα αρχεία ή φωτογραφίες
- ΔΕΝ απαντάμε, ιδίως αν ο παραλήπτης δεν ανήκει στις επαφές μας
- ΕΑΝ εντοπίσουμε ορθογραφικά, συντακτικά ή εκφραστικά λάθη, ΕΑΝ μας ζητείται να κάνουμε κάτι κατεπειγόντως, ΕΑΝ μας προσφέρεται κάτι που δεν έχουμε ζητήσει κλπ, είμαστε υποψιασμένοι οτι πιθανότατα πρόκειται για phishing ή άλλη μορφή απάτης.
- ΕΑΝ στο ύποπτο e-mail αναφέρεται κάποιο πρόσωπο, εταιρεία ή φορέας που γνωρίζουμε ή με τους οποίους συνεργαζόμαστε, φροντίζουμε να τους ενημερώσουμε, ώστε να προβούν στις αναγκαίες ενέργειες.
- ΕΑΝ υπάρχει σχετικός Κανονισμός στο Τμήμα μας (τί κάνουμε σε περίπτωση ύποπτου e-mail), ακολουθούμε τις οδηγίες, διαφορετικά καλούμε την Τεχνική Υποστήριξη.



Προσοχή: Αγαπητέ κάτοχο email!

Mrs.Kristalina Georgieva <oshiwish@gmail.com> Πέμ 30 Δεκ 2021, 5:50 π.μ. (πριν από 5 ημέρες)
προς κρυφή κοιν.: εγώ

Προσοχή: Αγαπητέ κάτοχο email!

Καλώς ήρθατε στο επίσημο e-mail του I.M.F. ΚΥΡΙΑ. ΔΙΕΥΘΥΝΤΗΣ. ΚΡΥΣΤΑΛΛΙΝΑ ΓΕΩΡΓΙΕΒΑ. Η ΕΚΘΕΣΗ ΜΑΣ: UBT (UNION BANK OF TOGOLESE)

Είμαι η κυρία Kristalina Georgieva, Διευθύντρια και Πρόεδρος (IMF) της Akodessewa-Togo. Θα θέλαμε να σας ενημερώσουμε ότι το Διεθνές Νομισματικό Ταμείο (ΔΝΤ) στην Ουάσιγκτον, DC, ΗΠΑ επισκέφτηκε τη χώρα μας για να μελετήσει τη διερεύνηση διαδικτυακής απάτης. Λάβατε αυτές τις πληροφορίες σήμερα επειδή η διεύθυνση ηλεκτρονικού ταχυδρομείου σας βρέθηκε στη λίστα των θυμάτων απάτης σε αυτήν τη χώρα.

Πρόσθετες πληροφορίες (IMF), Washington, DC. αποζημιώνει όλες τις χώρες που ήταν απατεώνες στη χώρα μας και η διεύθυνση email σας βρέθηκε σε αυτές τις λίστες θυμάτων. Ετσι! Η τράπεζά μας έχει εμπιστευθεί (ΔΝΤ) τη μεταφορά του κεφαλαίου αποζημίωσής σας με τη χρήση μεθόδων ΚΑΡΤΑΣ ΑΤΜ ή ΕΜΒΑΣΜΑΤΟΣ.

Παρατηρήσαμε ότι ορισμένοι κουκουλοφόροι/απατεώνες χρησιμοποιούν το όνομα αυτής της τράπεζας για να μιμηθούν τα χρήματα και να αποτρέψουν χρήματα και να αποτρέψουν τα χρήματα των πελατών μας. Σε αυτήν την περίπτωση, θα σας συμβουλεύσουμε να αγνοήσετε οποιαδήποτε επικοινωνία μέσω email/τηλεφώνου με οποιονδήποτε/οργανισμό που ισχυρίζεται ότι να έχετε στην κατοχή σας το ταμείο σας.

Ωστόσο, αποφασίσαμε να μεταφέρουμε αυτό το κεφάλαιο στο λογαριασμό σας στο ποσό των 1.500.000,00 $ (Ένα εκατομμύριο πεντακόσιες χιλιάδες δολάρια) χρησιμοποιώντας μια κάρτα Visa ATM ή τις μεθόδους WIRE TRANSFER. Δεν θα μπορέσουμε να πραγματοποιήσουμε αυτήν την πληρωμή χρησιμοποιώντας μόνο τη διεύθυνση email σας.
Θα επεξεργαστούμε δεόντως την αίτησή σας για την απαίτηση του κεφαλαίου σας και οι διακανονισμοί θα γίνουν κατόπιν πιστοποίησης και επαλήθευσης των στοιχείων σας ανάλογα, καθώς έχουμε στην κατοχή μας τα μέσα πληρωμών για το ποσό των 1.500.000,00 δολαρίων σε εσάς. Δεν μπορούμε να κάνουμε τίποτα από αυτήν τη στιγμή χωρίς να λάβουμε κάποιες απαραίτητες πληροφορίες από εσάς, όπως ορίζεται στα τραπεζικά μας πρωτόκολλα λειτουργίας και για το σκοπό αυτό, θέλουμε να διαβάσετε προσεκτικά και να συμπληρώσετε τις κατάλληλες πληροφορίες στα παρακάτω κενά για να διευκολύνετε την άμεση επεξεργασία των αξιώσεών σας ανάλογα.
Τώρα πρέπει να επιλέξετε μία από τις 2 παρακάτω επιλογές, αφού θέλετε να αποκτήσετε το χρηματικό έπαθλο σας;

Ενεργοποιήστε τα Windows
Μεταβείτε στις Ρυθμίσεις για να ενεργοποιήσετε τα Windo

8. Κινητά

Από τη στιγμή που τα κινητά έγιναν μέρος της καθημερινότητάς μας, έγιναν επίσης στόχος κάθε λογής απατεώνων. Θεωρητικά δεν αποτελούν αντικείμενο αυτού του οδηγού, επειδή δεν προσφέρονται από την υπηρεσία μας, αλλά στην πράξη είμαστε συχνά αναγκασμένοι να τα χρησιμοποιούμε, άλλοτε για την εργασία μας κι άλλοτε σε συνδυασμό με αυτήν. Ας μην ξεχνάμε οτι σε αυτά αποθηκεύουμε κάθε λογής εμπιστευτικές πληροφορίες, τόσο μέσω των διαφόρων εφαρμογών (apps) όσο και "χειροκίνητα" σε αρχεία κειμένου, SMS, φωτογραφίες κλπ.
Εξαιρώντας την περίπτωση να έχει πραγματικά μολυνθεί το κινητό μας από κάποιο μικρόβιο (ιό), οπότε το μόνο που μπορούμε να κάνουμε είναι να το δώσουμε σε κάποιον ειδικό για επισκευή, οι πιο συχνοί κίνδυνοι που θα αντιμετωπίσουμε με το κινητό είναι οι απάτες, παρόμοιες με εκείνες που διαπράττονται με e-mail. Εδώ βλέπουμε τις πιο συνηθισμένες από αυτές.

8.1 Αναπάντητες Κλήσεις

Δεχόμαστε κλήσεις από άγνωστο αριθμό, που διαρκούν ελάχιστα, ίσα ίσα για ένα κουδούνισμα. Σκοπός του απατεώνα είναι να καλέσουμε πίσω (για να δούμε ποιος ήταν ή τί ήθελε), οπότε μπορεί να δρομολογηθεί η κλήση μας σε αριθμό με ειδική χρέωση τύπου 090 και να καταλήξουμε με ένα φουσκωμένο λογαριασμό.

8.2 Τηλεφωνικό Phishing (Vishing)

Μας καλεί κάποιος προσποιούμενος οτι εκπροσωπεί κάποια υπηρεσία ή κάποια γνωστή εταιρεία, αρχικά για να κερδίσει την εμπιστοσύνη μας. Με διάφορους τρόπους προσπαθεί να μας πείσει να δώσουμε προσωπικά στοιχεία, πχ "πρέπει να κάνω επαλήθευση των στοιχείων σας" ή να κάνουμε κάποια συναλλαγή με χρήματα. Ένα στοιχείο αναγνώρισης αυτής της μορφής απάτης είναι οτι μας ζητούν να ενεργήσουμε κατά τη διάρκεια της κλήσης κι όχι να καλέσουμε αργότερα την όποια υπηρεσία ή τον όποιο ενδιαφερόμενο: τα στοιχεία μας "τώρα", μια πληρωμή "τώρα" κλπ.

8.3 SMS Phishing (Smishing)

Λαμβάνουμε ένα SMS που μοιάζει να είναι από κάποιο γνωστό μας ("καλησπέρα, γύρισα χθες από Λονδίνο, να κεράσω ένα καφέ το απόγευμα να τα πούμε από κοντά;") αλλά ο αριθμός του αποστολέα δεν αναγνωρίζεται. Σκοπός του επίδοξου απατεώνα είναι είτε να απαντήσουμε με SMS ή να τον καλέσουμε, να δούμε ποιος ήταν ο αποστολέας. Σε κάθε περίπτωση, είτε θα χρεωθούμε για κλήση σε "κόκκινο" αριθμό (τύπου 090) ή θα εγγραφούμε σε κάποια λίστα και θα λαμβάνουμε εν αγνοία μας μηνύματα με χρέωση.

8.4 Ηχογραφημένα Μηνύματα

Μας καλούν να μας ενημερώσουν για οτιδήποτε, συνήθως οτι κάτι κερδίσαμε, και μας ζητούν να κάνουμε κάποια ενέργεια, συνήθως μια κλήση σε άγνωστο αριθμό, για να διεκδικήσουμε το βραβείο-δώρο-οτιδήποτε. Αν καλέσουμε, είτε θα χρεωθούμε για κλήση σε "κόκκινο" αριθμό είτε θα εγγραφούμε εν αγνοία μας σε κάποια λίστα με ήχους κλήσης (τους οποίους θα λαμβάνουμε τακτικά, με ανάλογη χρέωση).

8.5 Ήχοι Κλήσεων

Σήμερα, ελάχιστες τίμιες επιχειρήσεις προσφέρουν ήχους κλήσεις για κινητά, αφού είναι πολύ απλό να τους διαμορφώσουμε χωρίς καμία ειδική υπηρεσία. Οι επίδοξοι απατεώνες μας προσφέρουν "σχεδόν δωρεάν" ήχους κλήσης, τους οποίους μας στέλνουν τακτικά (ίσως και

πολλές φορές τη μέρα) και μας χρεώνουν χωριστά για κάθε αποστολή ήχου. Κάποιες φορές μάλιστα, μας δυσκολεύουν για τη διακοπή αυτής της "υπηρεσίας".

8.6 Ασφάλεια Τηλεφώνου

Αν αποκτήσαμε πρόσφατα νέα συσκευή, είναι πιθανόν να μας καλέσουν προσφέροντάς μας ασφάλεια κινητού, δήθεν από το κατάστημα που κάναμε την αγορά ή από την εταιρεία κινητής. Στην καλύτερη περίπτωση θα αγοράσουμε μια κακής ποιότητας, αν όχι άχρηστη, ασφάλιση και στη χειρότερη θα πληρώσουμε για αέρα κοπανιστό.

Καλές πρακτικές στο κινητό

- Για το internet banking χρησιμοποιούμε αποκλειστικά την εφαρμογή της τράπεζάς μας.
- Κατεβάζουμε εφαρμογίδια (apps) αποκλειστικά από επίσημες πηγές, όπως τα Apple iTunes και Android Marketplace.
- Ενημερώνουμε το λειτουργικό του κινητού μας με κάθε νέα έκδοση.
- Κλειδώνουμε πάντα το κινητό με PIN που δεν γνωστοποιούμε σε κανέναν.
- Χρησιμοποιούμε προγράμματα προστασίας από ιούς μόνο εφόσον προέρχονται από επίσημο και αξιόπιστο κατασκευαστή.
- Ποτέ δεν πατάμε συνδέσμους σε κείμενα ή emails, εκτός αν (α) είμαστε απολύτως βέβαιοι για τον αποστολέα τους και (β) γνωρίζουμε πού θα μας οδηγήσουν.
- Μηνύματα που μας ενημερώνουν οτι κάτι πολύ καλό ή πολύ κακό συνέβη και πρέπει να κάνουμε κάτι (πχ να καλέσουμε ένα αριθμό), ΔΕΝ τα απαντάμε και ΔΕΝ καλούμε τον αριθμό, εκτός αν μπορούμε να επαληθεύσουμε τη γνησιότητα τόσο του αποστολέα όσο και του κειμένου.
- Ποτέ δεν δίνουμε προσωπικά ή άλλα εμπιστευτικά στοιχεία με SMS – κανένας αξιόπιστος φορέας ή επιχείρηση δεν ζητάει τέτοιες πληροφορίες με SMS.

Εάν εντοπίσατε κάποιο λάθος ή παρατυπία, εάν κάτι δε σας άρεσε, εάν θέλετε να προστεθεί κάτι ακόμη, εάν τελικά έχετε οποιαδήποτε παρατήρηση που μπορεί να βελτιώσει αυτό τον οδηγό, πείτε το σε εμάς, στέλνοντας ένα e-mail στη διεύθυνση που φαίνεται στο υποσέλιδο. Εάν κάτι σας άρεσε, εάν βρήκατε χρήσιμο τον οδηγό αυτό, εάν έχετε ένα καλό σχόλιο, πείτε το σε εμάς και μοιραστείτε τον οδηγό με τις φίλες και τους φίλους σας.

** Οι απειλές ταξινομήθηκαν με βάση τις σχετικές οδηγίες του Υπουργείου Εμπορίου των ΗΠΑ, τις μετρήσεις της Norton κλπ και προσαρμόστηκαν στην ελληνική πραγματικότητα από το συγγραφέα . Η φωτογραφία του εξωφύλλου και οι άλλες εικόνες είναι του συγγραφέα, εκτός από τη φωτογραφία με το λουκέτο και την οθόνη του Outlook, που είναι ελεύθερα διαθέσιμες στο διαδίκτυο. Ο Αλόμπαρ είναι ο ήρωας του βιβλίου "Το άρωμα του ονείρου" (Jitterbug Perfume) του Τομ Ρόμπινς. Το "42" είναι η απάντηση στο ερώτημα για τη ζωή, το σύμπαν και τα πάντα, από το βιβλίο "Γυρίστε το γαλαξία με οτοστόπ" του Ντάγκλας Άνταμς.

** Ο Βασίλης Τερζόπουλος ξεκίνησε την ενασχόλησή του με τους υπολογιστές ερασιτεχνικά, το 1985. Από το 1987 γράφει για εφαρμογές, επικοινωνία και ασφάλεια στον ψηφιακό χώρο, αρχικά σαν συντάκτης στο περιοδικό Pixel και στη συνέχεια σε διάφορα έντυπα και ψηφιακά μέσα. Από το 1993, με την εμπορική διάθεση του internet στην Ελλάδα, ασχολείται με αυτό επαγγελματικά (έρευνα και ανάπτυξη).

ΔΕΚΑΛΟΓΟΣ ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ

Μπήκε κάποιος στο γραφείο μου και έκατσε στον υπολογιστή μου να γράψει κάτι. Εν αγνοία μου έστειλε τρομοκρατικό e-mail και διώκομαι ποινικά.

1. Έχω πάντα κωδικό για να συνδεθώ στον υπολογιστή μου.

2. Έχω προστασία οθόνης, αυτόματα στα 5 λεπτά, με κωδικό.

3. Ενεργοποιώ την προστασία οθόνης κάθε φορά που απομακρύνομαι από τον υπολογιστή μου.

4. Δεν επιτρέπω σε κανέναν να χρησιμοποιήσει τον υπολογιστή μου, εκτός από άτομα ΚΑΙ γνώριμα ΚΑΙ εξουσιοδοτημένα.

Χάλασε ο σκληρός δίσκος κι έχασα τα έγραφά μου. Τα έχω χαμένα.

5. Στο τέλος κάθε ημέρας, κρατάω αντίγραφα ασφαλείας της δουλειάς μου.

Πάτησα κάπου στο ίντερνετ και κόλλησε ο υπολογιστής. Δεν ξέρω τί να κάνω.

6. Δεν πατάω "ό,τι να'ναι" στο ίντερνετ, εκτός εάν γνωρίζω πού θα οδηγηθώ.

Έλαβα e-mail οτι η Τράπεζά μου αυτό κι αυτό ή οτι κάποιος ζητάει ή χαρίζει χρήματα.

7. Ποτέ δεν πατάω συνδέσμους σε ασυνήθιστα e-mails.

Ο Δήμαρχος ή ο Τεχνικός ζήτησε τον κωδικό μου και του τον είπα. Την πάτησα μεγαλοπρεπώς.

8. Ποτέ και σε κανέναν δεν αποκαλύπτω τους κωδικούς μου.

Έκανα τσατ με φιλικό πρόσωπο κι έλεγα τα προσωπικά μου. Την επόμενη μέρα τα ήξεραν όλοι.

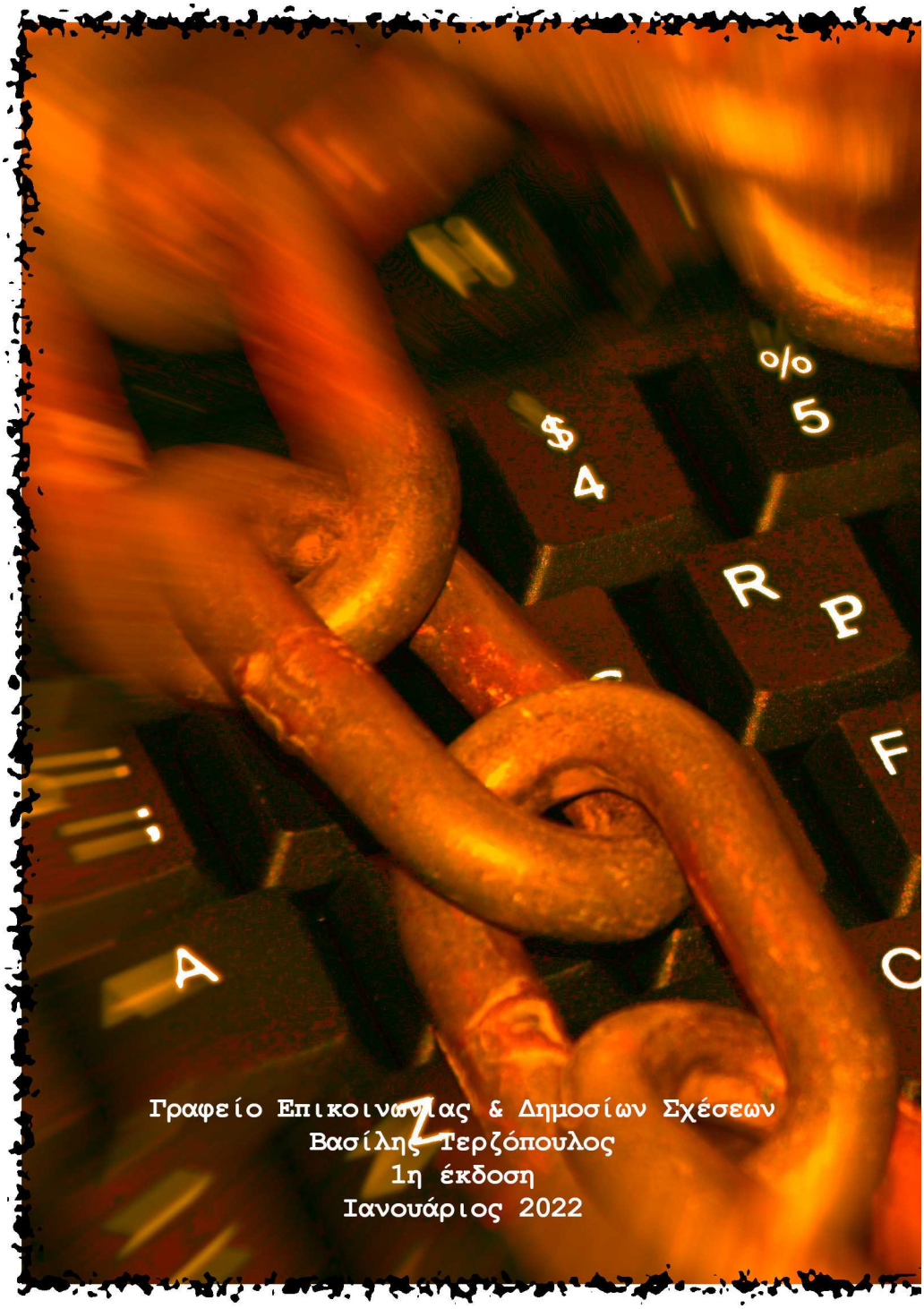
9. Τόσο στην πραγματική όσο και στην ψηφιακή ζωή, μπορεί κάποιος να κρυφακούει.

Κάτι πήγε στραβά αλλά εγώ τα έκανα όλα σωστά.

10. Όταν κάτι δεν πάει καλά, κάτι έκανα λάθος, κατά 99%.
Συνήθως επειδή "δεν το ήξερα" ή "πού να το φανταστώ".

Έξτρα:

10+1. Αν εντοπίσω πρόβλημα στον υπολογιστή ή στο ίντερνετ, δεν παίρνω πρωτοβουλίες για να μην χειροτερέψει το τυχόν πρόβλημα. Καλώ αμέσως την υποστήριξη.



Γραφείο Επικοινωνίας & Δημοσίων Σχέσεων
Βασίλης Τερζόπουλος
1η έκδοση
Ιανουάριος 2022