Η χρησιμότητα του Διαχειριστή Κωδικών Πρόσβασης (Password Manager)

Ένας διαχειριστής κωδικών πρόσβασης αποθηκεύει με ασφάλεια όλους τους ισχυρούς, μοναδικούς κωδικούς πρόσβασης για όλους τους λογαριασμούς στο διαδίκτυο. Πώς λειτουργεί; Αντιγράφετε τον κωδικό πρόσβασης από τον διαχειριστή κωδικών ή ο διαχειριστής κωδικών εισάγει αυτόματα τον κωδικό για τον ζητούμενο λογαριασμό.

Πώς να χρησιμοποιήσετε ασφαλώς το email σε μια φορητή συσκευή

- Πάνω από το 50% όλων των email ανοίγονται σε φορητή συσκευή, επομένως χρειάζεται να τη θωρακίσουμε.
- Βεβαιωθείτε ότι έχετε ορίσει έναν ασφαλή κωδικό πρόσβασης συσκευής. Ιδανικά, μπορείτε να χρησιμοποιήσετε έναν συνδυασμό γραμμάτων και αριθμών ή ακόμα και μια φράση πρόσβασης (μια φράση που μπορείτε εύκολα να απομνημονεύσετε είναι ένα πολύ ασφαλέστερο κλειδί συσκευής από μια μεμονωμένη λέξη).
- Αποφύγετε τα μη ασφαλή δωρεάν δημόσια Wi-Fi. Η σύνδεση μπορεί να είναι ανασφαλής και η επισκεψιμότητά σας στο διαδίκτυο θα μπορούσε να είναι ευάλωτη σε επιθέσεις. Οποιοσδήποτε με πρόσβαση στο δημόσιο Wi-Fi θα μπορούσε να παρακολουθεί τις ενέργειές σας και να αποκτήσει πρόσβαση στα προσωπικά σας δεδομένα.

- Εάν πρέπει να χρησιμοποιήσετε ένα μη ασφαλές δωρεάν Wi-Fi, η χρήση ενός εικονικού ιδιωτικού δικτύου (VPN) είναι ένα ζωτικό βήμα ασφάλειας. Η χρήση ενός VPN δημιουργεί μια ιδιωτική "σήραγγα" μεταξύ της συσκευής σας και του διακομιστή παροχής VPN, διασφαλίζοντας ότι κανείς δεν μπορεί να κατασκοπεύσει τα δεδομένα σας.
- Πραγματοποιείστε τακτικές σαρώσεις κατά του κακόβουλου λογισμικού (virus scan).
- Ενημερώστε το σύστημά σας εγκαθιστώντας τα τελευταία updates.
- Ενεργοποιήστε τον έλεγχο ταυτότητας 2 παραγόντων. Ο έλεγχος ταυτότητας 2 παραγόντων, ή 2FA, προσθέτει ένα επιπλέον επίπεδο ασφαλείας στον λογαριασμό σας, στέλνοντας έναν κωδικό περιορισμένης χρήσης σε μια συσκευή, τον οποίο πρέπει να εισάγετε.
- Προσθήκη κρυπτογράφησης. Εάν ο τρέχων πάροχος email δεν υποστηρίζει πρόσθετα επίπεδα κρυπτογράφησης, εξετάστε το ενδεχόμενο αλλαγής παρόχου. Εάν αυτό δεν είναι μια επιλογή, ένα επιπλέον βοηθητικό πρόγραμμα κρυπτογράφησης είναι αυτό που χρειάζεστε.

Τι είναι ο έλεγχος ταυτότητας δύο παραγόντων (2FA) και πώς τον χρησιμοποιείτε;

Ο έλεγχος ταυτότητας δύο παραγόντων (2-FA) είναι μια σημαντική πρόσθετη δυνατότητα διασφάλισης λογαριασμού email. Το 2FA είναι μια διαδικασία που απαιτεί να εισαγάγετε δύο διαφορετικούς κωδικούς πρόσβασης για να ξεκλειδώσετε τον λογαριασμό σας. Η πρώτη επαλήθευση είναι ο μοναδικός κωδικός πρόσβασής σας. Η δεύτερη επαλήθευση είναι ένας κωδικός περιορισμένου χρόνου που αποστέλλεται σε συσκευή της επιλογής σας. Ωστόσο μπορείτε να χρησιμοποιήσετε δακτυλικό αποτύπωμα ή άλλη βιομετρική σάρωση στη θέση του. Η ιδέα είναι ότι μόνο ο ιδιοκτήτης του νόμιμου λογαριασμού θα πρέπει να έχει πρόσβαση στο δεύτερο κομμάτι των δεδομένων επαλήθευσης, αυξάνοντας δραστικά το επίπεδο ασφαλείας. Για παράδειγμα, όταν συνδέεστε στον λογαριασμό email σας, εισάγετε τον ασφαλή κωδικό πρόσβασής σας. Επειδή έχετε το 2-FA ενεργοποιημένο, λίγα λεπτά αργότερα λαμβάνετε έναν εξαψήφιο κωδικό που πρέπει να εισαγάγετε στον πίνακα σύνδεσης πριν λήξει ο κωδικός. Χωρίς τον δεύτερο κωδικό, ο λογαριασμός email σας παραμένει κλειδωμένος.

CYBER ALERT
ΔΙΩΞΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ
11188

ΕΠΙΚΟΙΝΩΝΙΑ

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος – Cyber Crime Division
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11522
e-mail: ccu@cybercrimeunit.gov.gr, Τηλ.:11188, Fax: 2131527471

Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδας
Μοναστηρίου 326, Τ.Κ. 54 121 Θεσσαλονίκη
e-mail: ydheve@cybercrimeunit.gov.gr, Τηλ.:11188, Fax: 2131527666

Ενημερωθείτε για θέματα ασφαλούς πλοήγησης στο Διαδίκτυο στο
https://www.cyberkid.gov.gr και στο https://www.cyberalert.gr

Για άμεση ενημέρωση που αφορά θέματα της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος ακολουθήστε μας στα μέσα κοινωνικής δικτύωσης:

https://www.facebook.com/cyberkid.gov.gr/
https://www.facebook.com/CyberAlertGR/
https://www.instagram.com/cyberalert.gr/
https://twitter.com/CyberAlertGR
Youtube channel: Cyber Alert

Τα νερά δεν είναι πάντα ασφαλή.
Σέρφαρε με προσοχή.

Ασφάλεια για όλους
Ασφάλεια **στο διαδίκτυο**

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Προστασίας του Πολίτη

Αρχηγείο Ελληνικής Αστυνομίας

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Συμβουλές διασφάλισης email

Όλοι μας χρειαζόμαστε ασφαλές email!

Το προστατευμένο email είναι το πρώτο και πιο σημαντικό βήμα για την ασφάλεια στο διαδίκτυο!

- Κάθε φορά που εγγράφεστε σε μια νέα online υπηρεσία, χρησιμοποιείτε το email σας.
- Όταν ξεχνάτε ένα password, χρησιμοποιείτε το email σας για να το επαναφέρετε.
- Στο inbox έχετε διευθύνσεις, αριθμούς τηλεφώνου, προσωπικές πληροφορίες και πολλά ακόμα.

Ενδιαφέροντα στοιχεία

- Το ηλεκτρονικό ταχυδρομείο είναι ένα από τα κορυφαία εργαλεία επικοινωνίας για τις επιχειρήσεις.
- Ο μέσος υπάλληλος γραφείου λαμβάνει πάνω από 120 emails κάθε μέρα και στέλνει 40.
- Το 86% των επαγγελματιών δηλώνουν το email είναι το αγαπημένο τους εργαλείο επικοινωνίας, ενώ το 66% των πολιτών διαβάζουν emails στις ψηφιακές τους συσκευές.

Πώς μπορεί κάποιος να υποκλέψει τα emails σας:

- Μέσω της συσκευής, στην οποία διαβάζετε τα email σας, όπως το smartphone ή το desktop.
- Μέσω της σύνδεσης διαδικτύου που χρησιμοποιείτε για να έχετε πρόσβαση στον λογαριασμό σας.
- Μέσω του server που εξυπηρετεί το email σας.
- Μέσω της συσκευής του παραλήπτη, από όπου διαβάζει τα email του.

Συνηθισμένα λάθη

- Μήπως ακολουθείτε links ή ανοίγετε attachments που περιέχονται σε ύποπτα emails; Μέσω αυτών μπορεί να εγκατασταθεί κακόβουλο λογισμικό.
- Πιθανόν δεν έχετε ενεργοποιήσει το φίλτρο spam emails.
- Ενδεχομένως χρησιμοποιείτε αδύναμα και επαναχρησιμοποιούμενα passwords.

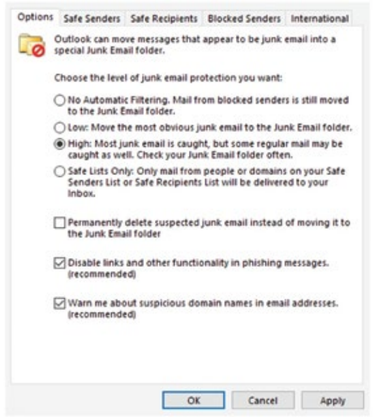
Πώς αντιλαμβανόμαστε τα ύποπτα scam και phishing emails;

Υπάρχουν τα παρακάτω πέντε βήματα που μπορείτε να κάνετε για να εξετάσετε γρήγορα αν το email που σας ήρθε είναι αληθές.

1. Ελέγξτε προσεκτικά τη διεύθυνση email του αποστολέα.
2. Ελέγξτε την ορθογραφία του email.
3. Το email περιέχει τη λέξη «ΕΠΕΙΓΟΝ»
4. Το email περιέχει attachments.
5. Το email περιέχει links.

Ενεργοποιείστε το spam φίλτρο

Ο λογαριασμός email έχει spam φίλτρο. Το φίλτρο ελέγχει τα εισερχόμενα emails για spam διευθύνσεις, spam περιεχόμενο, spam θέμα και κακόβουλα συνημμένα. Αν εντοπίσει ένα τέτοιο email, το στέλνει κατευθείαν στο spam box. Η ενεργοποίησή του πραγματοποιείται μέσω της εφαρμογής διαχείρισης email που χρησιμοποιείτε.



Συμβουλές για δυνατούς κωδικούς στους λογαριασμούς

- Ο κωδικός πρέπει να είναι τουλάχιστον δώδεκα χαρακτήρες.
- Θα πρέπει να χρησιμοποιείτε έναν συνδυασμό γραμμάτων (κεφαλαίων - μικρών), αριθμών και συμβόλων.
- Ιδανικά μπορείτε να χρησιμοποιήσετε μια «φράση πρόσβασης» αντικαθιστώντας κάποια γράμματα με σύμβολα και αριθμούς.
- Δεν πρέπει να χρησιμοποιείτε στοιχεία αναγνώρισης: γενέθλια, ονόματα κατοικίδιων ζώων, τόπους γέννησης κ.λπ.

Ένας ιδανικός κωδικός πρόσβασης θα μπορούσε να μοιάζει με τον ακόλουθο: **Zwb2=<UwrP77”?ra**