Security tips για την Email υπηρεσία.

- 2022-10-21 - Troubleshooting / Spam

Η ασφάλεια του Διαδικτύου είναι ένα θέμα που όλοι γνωρίζουμε ότι είναι σημαντικό, αν όχι το σημαντικότερο, αλλά συχνά βρίσκεται στις εσοχές του μυαλού μας, πλανώντας τον εαυτό μας να πιστέψει ότι «δεν θα συμβεί σε μένα». Είτε πρόκειται για την καταστροφική δύναμη ενός νέου ιού ή απλώς για προσπάθειες hacking, είμαστε πάντοτε μόνο ένα κλικ μακριά από το να αντιμετωπίσουμε ένα χάος ασφάλειας.

Οι ασφαλείς διαδικτυακές πρακτικές είναι σημαντικές για να διατηρήσετε την ηλεκτρονική σας ταυτότητα αναλλοίωτη και απαλλαγμένη από ιούς, χάκερς και όλα τα είδη διαδικτυακών απειλών. Και το καλύτερο μέρος για να ξεκινήσετε; Τα εισερχόμενά σας.

Ακολουθούν μερικές απλές αλλά σημαντικές συμβουλές ασφαλείας που πρέπει να γνωρίζετε για να διατηρήσετε όσο το δυνατόν πιο ασφαλή τον λογαριασμό σας ηλεκτρονικού ταχυδρομείου.

1. Ισχυρό password.

Ο κωδικός σας (password) πρέπει να αποτελείται από γράμματα (κεφαλαία και πεζά), αριθμούς και σύμβολα, να αποτελείται τουλάχιστον από 8 έως 12 χαρακτήρες και να τον αλλάζετε σε τακτά χρονικά διαστήματα.

TIP : Μην χρησιμοποιείτε τον ίδιο κωδικό σε email, social media και άλλες διαδικτυακές υπηρεσίες.

2. Προσοχή στις απάτες (Spam/Phishing).

Όταν ασχολείστε με μια συγκεκριμένη εταιρεία ή ένα προϊόν που απαιτεί πληροφορίες λογαριασμού, λογικά θα έχετε δει το εξής μήνυμα: "Ποτέ μην δίνετε τα προσωπικά σας στοιχεία. Ποτέ δεν θα σας ζητήσουμε τον κωδικό πρόσβασής σας. "Όταν κάποιος σας στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που σας ζητάει τα προσωπικά σας στοιχεία, γνωρίζετε αμέσως ότι είναι ένα τέχνασμα - Spam.

Αλλά υπάρχει ένα άλλο επίπεδο σε αυτήν την απάτη και ονομάζεται phishing. Βασικά, οι κακόβουλοι χρήστες μιμούνται sites υψηλού προφίλ (π.χ. eBay, Amazon, Facebook κλπ) και

θα σας ενημερώνουν ότι αντιμετωπίζει προβλήματα ο λογαριασμός σας. Το μόνο που έχετε να κάνετε για να επιδιορθώσετε αυτό το πρόβλημα είναι να τους στείλετε το όνομα χρήστη και τον κωδικό πρόσβασής σας για να επαληθεύσετε την αυθεντικότητά σας. Μερικές φορές θα σας συνδέσουν με έναν ψεύτικο site που μοιάζει ακριβώς με το πραγματικό. Να είστε επιφυλακτικοί, να επικοινωνήσετε με την αντίστοιχη υποστήριξη του site που σας έχει "στείλει" το συγκεκριμένο email και να μην δίνετε ποτέ τα στοιχεία σας (Username/password).

3. Μην κάνετε κλικ σε όλα τα link.

Κάθε φορά που βλέπετε ένα σύνδεσμο σε ένα email, κατά 99% δεν πρέπει να κάνετε κλικ σε αυτό. Οι μόνες εξαιρέσεις είναι όταν περιμένετε ένα συγκεκριμένο μήνυμα ηλεκτρονικού ταχυδρομείου, όπως ένα σύνδεσμο εγγραφής φόρουμ ή ένα μήνυμα ηλεκτρονικού ταχυδρομείου ενεργοποίησης λογαριασμού.

Αν λάβετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου ανεπιθύμητης αλληλογραφίας που προσπαθεί να σας πουλήσει μια συγκεκριμένη υπηρεσία ή προϊόν, μην κάνετε κλικ σε κανέναν από τους συνδέσμους μέσα. Ποτέ δεν ξέρεις πού θα σας οδηγήσουν. Μερικές φορές μπορεί να είναι ασφαλείς. Άλλες φορές θα σας φέρουν αντιμέτωπους με κακόβουλα προγράμματα και ιούς.

Εάν λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από την τράπεζά σας ή οποιαδήποτε άλλη υπηρεσία (π.χ. πληρωμές λογαριασμών), επισκεφθείτε πάντα τον ιστότοπο με μη αυτόματο τρόπο (όχι μέσω του email σας).

4. Μην ανοίγετε συνημμένα αρχεία.

Τα συνημμένα είναι μία δύσκολη παράμετρος όταν πρόκειται για το ηλεκτρονικό ταχυδρομείο. Εάν περιμένετε κάτι από έναν φίλο ή από μία γνωστή σας επαφή, τότε σίγουρα, προχωρήστε και ανοίξτε το συνημμένο.

Εάν όμως το μήνυμα ηλεκτρονικού ταχυδρομείου δεν ζητηθεί, μην ανοίξετε ποτέ το/τα συνημμένα που περιέχει. Ακόμα κι αν το αρχείο φαίνεται "αθώο". Τα ονόματα αρχείων μπορούν να παραποιηθούν. Τα αρχεία JPEG θα μπορούσαν να είναι EXEs μέσω μετονομασίας/επεξεργασίας και αυτά τα EXEs θα τρέξουν αμέσως μόλις ληφθούν και πιθανό να είναι κακόβουλα.

5. Έλεγχος με Antivirus / Antimalware.

Εάν ανοίξετε ένα email και φαίνεται ύποπτο με οποιονδήποτε τρόπο, τρέξτε άμεσα ένα antivirus.

TIP : Να τρέχετε antivirus αλλά και malware scan στον υπολογιστή σας σε τακτά χρονικά διαστήματα. Βεβαιωθείτε πως τα Malware/Antivirus scan είναι αναβαθμισμένα και ενημερωμένα σε τελευταίες εκδόσεις.

6. Ελέγξτε τα φίλτρα σας μέσα από το webmail σας.

Κακόβουλα κάποιος μπορεί να συνδεθεί στο webmail σας και μέσω των φίλτρων να ενεργοποιήσει ανακατεύθυνση σε τρίτο δικό του λογαριασμό email. Οφείλετε σε τακτά χρονικά διαστήματα να ελέγχετε τα φίλτρα σας μέσα από το Webmail σας.

Σε περίπτωση που χρησιμοποιείτε το Horde -> Preferences -> Filters.
Σε περίπτωση που χρησιμοποιείτε το Roundcube -> Settings -> Filters.

7. Χρησιμοποιείτε θύρες με Encryption.

Σε περίπτωση που έχετε εγκαταστήσει το email σας σε mail client όπως το Outlook πχ, στην θύρα εξερχόμενης αλληλογραφίας δηλώστε θύρες που χρησιμοποιούν encryption όπως την 465 με SSL ή την 587 με TLS/SSL.