1. **Πώς μπορούμε να σερφάρουμε στο Internet με ασφάλεια αλλά και να δημιουργήσουμε ένα ασφαλές περιβάλλον κυβερνοχώρου για εμάς και την οικογένειά μας?**

- Βασικό μέρος της προστασίας του σπιτιού μας, είναι η εξασφάλιση του ασύρματου δικτύου μας WiFi
    - Αλλάζουμε τον εργοστασιακό κωδικό πρόσβασης. Ο κωδικός αυτός μας επιτρέπει να ρυθμίσουμε το ασύρματο δίκτυό μας. Ένας επιτιθέμενος μπορεί σχετικά εύκολα να ανακαλύψει τον κωδικό πρόσβασης που έχει θέσει ο κατασκευαστής.
    - Επιτρέπουμε μόνο σε ανθρώπους εμπιστοσύνης να συνδεθούν στο δικό μας δίκτυο
    - Δημιουργούμε "ισχυρούς" κωδικούς πρόσβασης που δύσκολα μπορούν να ανακτηθούν. Θυμηθείτε, χρειάζεται να εισαγάγετε τον κωδικό πρόσβασης μία φορά μόνο για κάθε μια από τις συσκευές σας.
    - Ελέγχουμε ποιες συσκευές συνδέονται στο οικιακό μας δίκτυο.
- Έχουμε πάντα εγκατεστημένο και ενημερωμένο ένα πρόγραμμα προστασίας από ιούς (Antivirus) σε όλες τις συσκευές.
- Χρησιμοποιούμε πάντα τις πιο πρόσφατες εκδόσεις λογισμικού, λειτουργικού συστήματος και εφαρμογών σε όλες τις συσκευές μας. Ορισμένες υπηρεσίες, όπως το GoogleChrome, ενημερώνονται αυτόματα ενώ άλλες ειδοποιούν τους χρήστες σχετικά με το πότε πρέπει να τις ενημερώσουν. Αυτός ο κανόνας ισχύει για σχεδόν οποιαδήποτε τεχνολογία που συνδέεται στο διαδίκτυο (mobile phones, tablets, TVs, κάμερες ασφαλείας, baby cameras και κονσόλες παιχνιδιών).
- Παίρνουμε συχνά αντίγραφα ασφαλείας (backup)

2. **Πώς Δημιουργούμε "ισχυρούς" κωδικούς πρόσβασης?**

- Χρησιμοποιούμε μοναδικούς, ισχυρούς κωδικούς πρόσβασης
- Ένα ισχυρό Password πρέπει να έχει τουλάχιστον 8 χαρακτήρες, Κεφαλαία και μικρά γράμματα, αριθμούς και ειδικούς χαρακτήρες
- Αλλάζουμε συχνά τους κωδικούς πρόσβασης (π.χ. κάθε 90 ημέρες)
- Δεν εμπιστευόμαστε σε κανέναν τους κωδικούς πρόσβασης σε κανέναν
- Ενεργοποιούμε, όπου είναι δυνατό, τον έλεγχο ταυτότητας δύο παραγόντων (two factor authentication) για επιπλέον επίπεδο ασφάλειας

3. **Πώς προστατευόμαστε από παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου (Phishing emails ή SMS)**

- Ελέγχουμε προσεκτικά την ηλεκτρονική διεύθυνση του αποστολέα του μηνύματος, παρατηρούμε το μήνυμα για ορθογραφικά λάθη και λάθη γραμματικής ή σύνταξης
- Είμαστε ιδιαίτερα προσεκτικοί εάν ένα μήνυμα μας ζητά ευαίσθητες πληροφορίες (π χ κωδικούς πρόσβασης της ηλεκτρονικής τραπεζικής internet banking, επιβεβαίωση αριθμού πιστωτικών καρτών)
- Δεν συμπληρώνουμε προσωπικά δεδομένα και δεν ενημερώνουμε τα στοιχεία μας σε links μέσω emails
- Προσέχουμε ιδιαίτερα όταν χρησιμοποιούμε φορητή συσκευή για παράδειγμα κινητό τηλέφωνο ή tablet, ενδεχομένως να είναι πιο δύσκολο να εντοπίσουμε απόπειρα phishing
- Όταν πρόκειται για ηλεκτρονικές συναλλαγές δεν επιλέγουμε links και δεν πραγματοποιούμε λήψη αρχείου (download) όταν προέρχονται από μηνύματα, αντίθετα πληκτρολογούμε την διεύθυνση του ηλεκτρονικού συνδέσμου στον browser που χρησιμοποιούμε ή συνδεόμαστε μέσω της επίσημης εφαρμογής (App).

4. **Πώς μπορούμε να κάνουμε αγορές στο Internet με ασφάλεια?**

- Πληκτρολογούμε την διεύθυνση του εμπόρου που έχουμε επιλέξει για τις αγορές στην γραμμή διευθύνσεων του Browser
- Βεβαιωνόμαστε ότι η ηλεκτρονική διεύθυνση του εμπόρου που έχουμε επιλέξει για τις αγορές μας ξεκινά με «https" και αναζητούμε το εικονίδιο κλειδώματος στη γραμμή περιήγησης του browser
- Δεν ψωνίζουμε μέσω μη ασφαλών δημόσιων δικτύων WiFi
- Χρησιμοποιούμε προπληρωμένες πιστωτικές κάρτες για μεγαλύτερη π[προστασία
- Δεν αποθηκεύουμε στοιχεία καρτών στους browsers
- Ελέγχουμε αν υπάρχει ξεκάθαρη πολιτική επιστροφών και αποστολής email με την αγορά του προϊόντος

Περισσότερες συμβουλές:

Συζητάμε με τα άλλα μέλη της οικογένειάς μας για τους κινδύνους του Internet, ενημερώνουμε τα παιδιά μας και τους γονείς μας για την ασφάλεια στο διαδίκτυο και ρυθμίζουμε τους ψηφιακούς κανόνες στο σπίτι μας.

Προσέχουμε τι κοινοποιούμε στα social media, προστατεύουμε το ψηφιακό μας προφίλ και το ψηφιακό μας αποτύπωμα

Παραμένουμε προσεκτικοί στην online δημόσια ζωή μας όσο και στην πραγματική.