



**DIGITAL SECURITY
AUTHORITY**

Ενημέρωση ασφαλείας για εργασία από το σπίτι

Εθνική Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων



Εισαγωγή

Αυτή η παρουσίαση αναφέρεται στη σημασία της ψηφιακής ασφάλειας των εξ αποστάσεως εργαζόμενων και τονίζει τις απλές τεχνικές που μπορούν να χρησιμοποιήσουν οι χρήστες για να προστατεύσουν τον εαυτό τους ενώ εργάζονται εξ αποστάσεως.

Η παρουσίαση χωρίζεται σε δύο τμήματα:

1. Κατανόηση της ανάγκης για ασφάλεια στην εργασία από το σπίτι
2. Βασικές πρακτικές ασφαλείας

Κατανόηση της ανάγκης για ασφάλεια στην εργασία από το σπίτι

Οι κίνδυνοι της εξ αποστάσεως εργασίας

- **Σειρά από κινδύνους που αφορούν**
 - Απώλεια ή κλοπή αντικειμένων (Laptop, Token, Mobile Phones)
 - Υποκλοπή πληροφοριών
 - Υποκλοπή στοιχείων χρήστη (credentials)
- **Μέθοδοι μείωσης κινδύνων**
 - Διαδικασίες
 - Τεχνικές
 - Εργαλεία



<https://www.le-vpn.com/covid-19-pandemic/>

DIGITAL SECURITY AUTHORITY

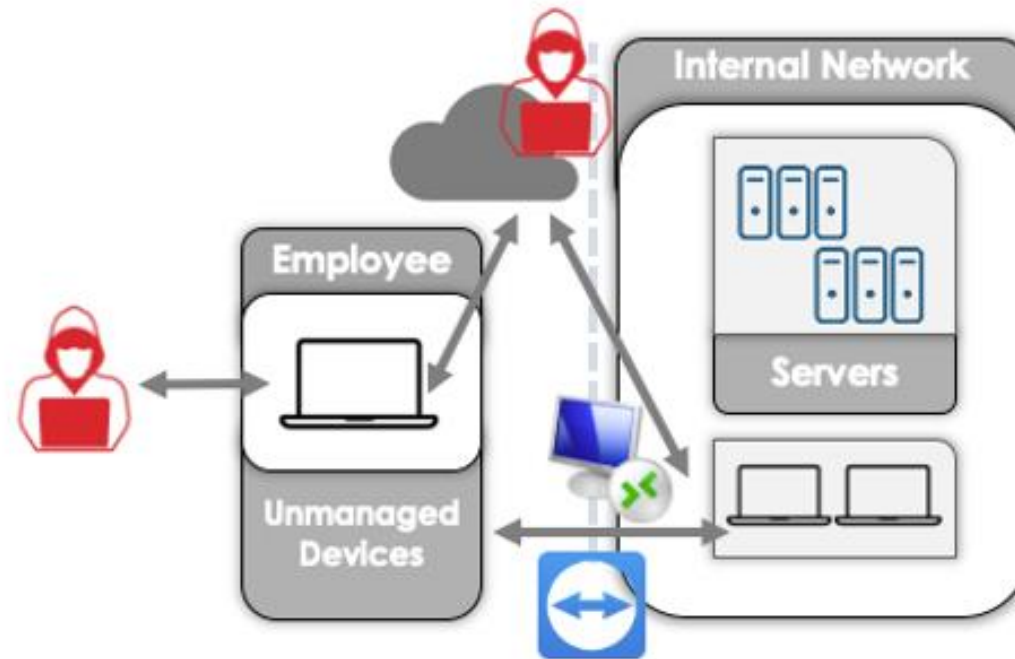
Κίνδυνοι μόλυνσης από κακόβουλο λογισμικό στα εργαλεία (laptops, tablet) που περιέχουν:

- Παιχνίδια (Video Games)
- Ταινίες
- Αρχεία Μουσικής



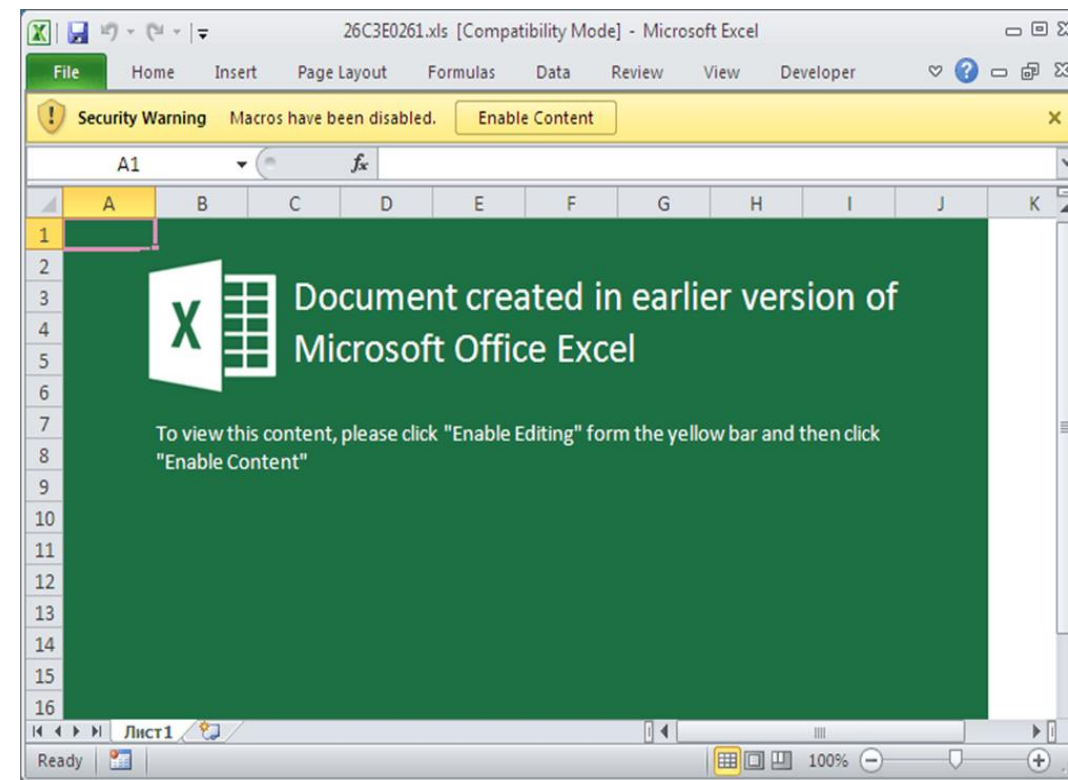
<https://www.flickr.com/photos/114267666@N06/22231287483/>

Παραδείγματα περιστατικών



Κακόβουλα Αρχεία

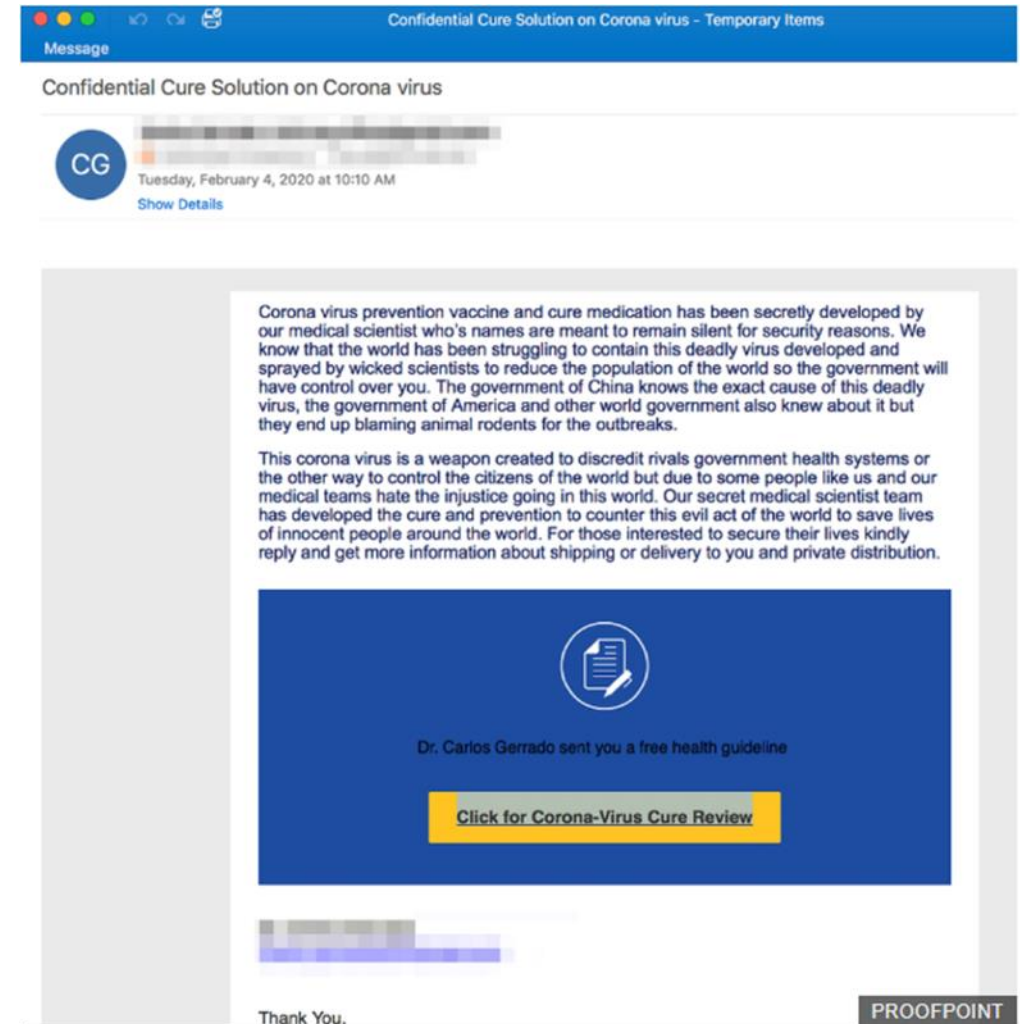
- Προσοχή σε μηνύματα ενεργοποίησης μακροεντολών.



<https://www.fortinet.com/blog/threat-research/microsoft-excel-files-increasingly-used-to-spread-malware.html>

Κακόβουλα μηνύματα σε κινητές συσκευές

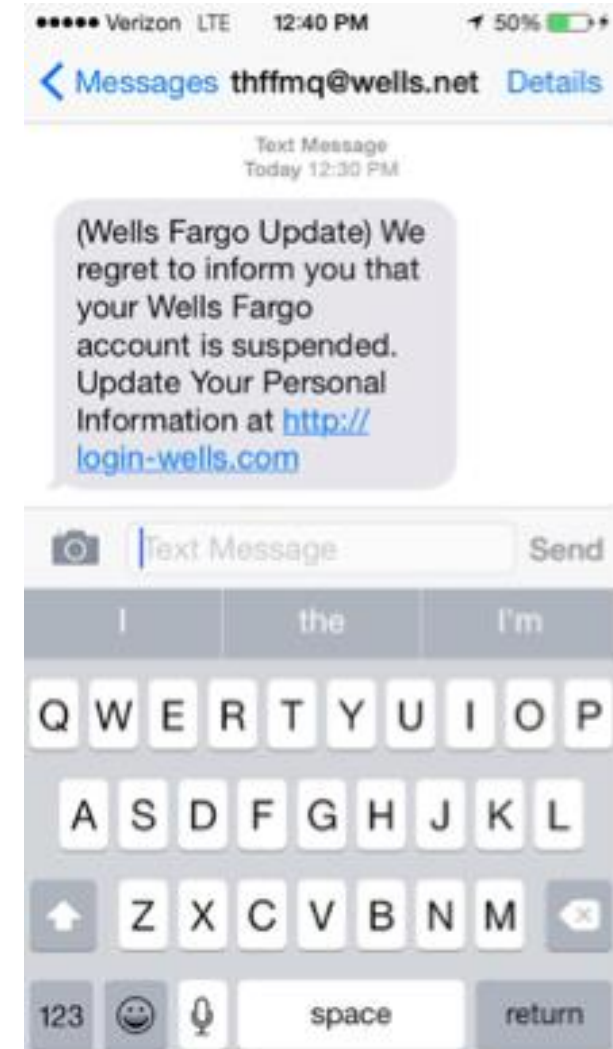
- Προστατευόμαστε από ψευδές ηλεκτρονικά μηνύματα.
- Επικοινωνία, με συναδέλφους και Administrators



<https://www.bbc.com/news/technology-51838468>

Παραπλανητικές διαφημίσεις

- Αποφυγή κακόβουλων μηνυμάτων σε κινητές συσκευές προσωπικές ή της υπηρεσίας.
- Ενημέρωση για καμπάνιες SMShing



Βασικές πρακτικές ασφαλείας



<https://ci.security/resources/news/article/8-best-practices-for-working-remotely>

Φυσική Ασφάλεια συσκευής

- Φύλαξη του εργασιακού υπολογιστή/κινητού τηλεφώνου σε ασφαλές μέρος (κατά προτίμηση κλειδωμένο).
- Χρήση του χαρακτηριστικού “Sleep Mode”



Κωδικοί

- Ασφαλής αποθήκευση των συνθηματικών χρηστών (Credentials)
- Απαγόρευση μεταφοράς, ανταλλαγής και διαμοιρασμού των συνθηματικών
- Επιλογή συνθηματικών που είναι σύμφωνα με τις προδιαγραφές ασφαλείας του οργανισμού
- Αποφυγή χρήσης του ίδιου συνθηματικού σε πολλαπλούς λογαριασμούς χρήστη

I changed
my password
to "incorrect"
so whenever
I forget what it is,
the computer will say
"your password is
incorrect."

Ασφάλεια συσκευής από μη εξουσιοδοτημένη πρόσβαση

- Σε καμία περίπτωση δεν πρέπει να φυλάσσονται προσωπικά δεδομένα και διαβαθμισμένα έγγραφα εκτός γραφείου.
- Ποτέ δεν δίνουμε πρόσβαση σε διαβαθμισμένες πληροφορίες σε τρίτους ή μη διαβαθμισμένους συναδέλφους.
- Ποτέ δεν ζητούμε τεχνική υποστήριξη από τρίτους όσο αφορά τις εργασιακές μας συσκευές

Ασφάλεια αρχείων εργασίας και προστασία συσκευής

- Ελέγχουμε συστηματικά για την ορθή λειτουργία του λογισμικού antivirus
- Αποφεύγουμε την σύνδεση εξωτερικών συσκευών (USB, Hard Disk, CD/DVD)
- Σύνδεση μόνο σε ασφαλή δίκτυα/Wi-Fi.
- ΠΟΤΕ δεν χρησιμοποιούμε public Wi-Fi ή οποιοδήποτε δίκτυο δεν είναι προστατευμένο από δυνατό κωδικό

Ασφάλεια αρχείων εργασίας και προστασία συσκευής

- Κρατάμε τον υπολογιστή ενημερωμένο (Windows Updates)
- Κατεβάζουμε από το εργασιακό δίκτυο μόνο τα απαραίτητα αρχεία για την καθημερινή εργασία
- Όλα τα αρχεία να φυλάσσονται στο δίκτυο και τους servers του οργανισμού.

Δίαυλος επικοινωνίας με System Administrator

- Έπαρξη ασφαλούς μεθόδου επικοινωνίας με τους αρμόδιους system administrators του οργανισμού σε περίπτωση τεχνικού σφάλματος ή ύποπτης ενέργειας.
- Έπαρξη άμεσης και εύχρηστης μεθόδου επικοινωνίας με τους αρμόδιους υπεύθυνους ασφαλείας σε περίπτωση ύποπτων ενεργειών

! Ένας sys admin δεν θα σας ζητήσει ποτέ τα στοιχεία πρόσβασης !

Πλάνο Επικοινωνίας

- Επικοινωνία από/προς τη Διοίκηση
- Επικοινωνία από/προς τους Υπαλλήλους
- Επικοινωνία από/προς Υπεύθυνους Ασφαλείας και Admins

Ανακεφαλαίωση

- Κατανόηση της ανάγκης για ασφάλεια στην εργασία από το σπίτι
- Παραδείγματα περιστατικών
- Βασικές πρακτικές ασφαλείας

Ενημέρωση για υφιστάμενες απειλές

- Επιπρόσθετα μπορείτε να επισκέπτεστε την ιστοσελίδα μας, όπου καθημερινά δημοσιεύονται υφιστάμενες απειλές
- <https://csirt.cy/>

Αναφορές

- https://cert.europa.eu/cert/newsletter/en/latest_PublicationsAndNewsletters_.html
- <https://csirt.cy/requirements-for-remote-work/>
- <https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home>
- <https://il-cert.org.il/>
- <http://www.securityfocus.com/infocus/1187>
- <http://technet.microsoft.com/en-us/windows/aa905065.aspx>
- <http://www.securityfocus.com/infocus/1186>
- <http://www.securityfocus.com/news/11393>
- <https://www.fortinet.com/blog/threat-research/microsoft-excel-files-increasingly-used-to-spread-malware.html>

Ευχαριστούμε!