Ενίσχυση της κυβερνοασφάλειας κατά την Τηλεργασία

Γιώργος Πράτσος

Σύμβουλος Τεχνητής Νοημοσύνης & Ψηφιακής Ασφάλειας

30/04/2026


Εταιρία:
ARUP
βασισμένη στο
Hong Kong
AI DEEPFAKE
Πότε:
Φεβρουάριος 2024
Μέθοδος:
Deepfake video call
$25.6 εκ.
15 εμβάσματα

Πώς θα αντιδρούσατε εσείς;

Γιατί πέτυχε η απάτη της Arup

1. Φανταστείτε ότι σας καλεί ο CFO σας σε βιντεοκλήση. Τον βλέπετε. Τον ακούτε. Είναι αυτός.

2. Φανταστείτε ότι στην κλήση είναι και δύο συνάδελφοι που γνωρίζετε. Όλοι συμφωνούν.

3. Φανταστείτε ότι σας ζητούν επείγουσα μεταφορά. Έχετε εξουσιοδότηση. Το έχετε ξανά κάνει.

4. Και όμως, δεν είναι αυτοί. Είναι μια τέλεια απάτη με deep fake και κοινωνική μηχανική.

Γιώργος Πράτσος

Σύμβουλος Τεχνητής Νοημοσύνης & Ψηφιακής Ασφάλειας

27+ έτη εμπειρίας στην Πληροφορική

18+ έτη εμπειρίας στην Εκπαίδευση

Εκπαιδευτής ΤΝ & Κυβερνοασφάλειας

Συνδεθείτε μαζί μου

linkedin.com/in/georgepratsos

Στο γραφείο, η ασφάλεια ήταν συλλογική.
Στο σπίτι, είναι ατομική.

Στο γραφείο

Ένα τείχος. Όλοι μέσα.

Στο σπίτι

Πολλές μικρές ασπίδες. Ο καθένας μόνος του.

ΣΗΜΕΙΑ ΕΥΠΑΘΕΙΑΣ ΤΗΛΕΕΡΓΑΣΙΑΣ ΚΑΤΟΙΚΙΑΣ

ΥΠΟΜΝΗΜΑ

ΟΙΚΙΑΚΟ WiFi - Default κωδικοί & παλιά firmware
Παρωχημένος εξοπλισμός ή ασθενής κρυπτογράφηση

ΚΟΙΝΟΧΡΗΣΤΕΣ ΣΥΣΚΕΥΕΣ
Πολλαπλοί χρήστες και IoT συσκευές αυξάνουν τον κίνδυνο

ΜΟΛΥΣΜΕΝΗ ΕΙΣΑΓΩΓΗ USB
Μη αξιόπιστα USB μπορεί να μεταφέρουν κακόβουλο λογισμικό

ΔΗΜΟΣΙΟ WiFi ΚΑΦΕΤΕΡΙΑΣ
Μη ασφαλή δίκτυα μπορεί να υποκλέψουν δεδομένα

Shadow IT/Χρήση μη εγκεκριμένων εφαρμογών
Μη εγκεκριμένες υπηρεσίες cloud εκθέτουν εταιρικά δεδομένα

Ο κίνδυνος στο σπίτι = ο κίνδυνος της εταιρείας

ΣΠΙΤΙ

Wi-Fi • Κωδικός • Phishing

ΕΤΑΙΡΕΙΑ

GDPR • Ransomware • Απάτη

Δεν υπάρχει "προσωπικό" λάθος στην τηλεργασία.

Οι 3 απειλές που χτυπάνε τους τηλεργαζόμενους

Phishing

πιο δύσκολο να συμβουλευτείτε συνάδελφο

Κλοπή κωδικών

Το οικιακό δίκτυο δεν είναι εταιρικό δίκτυο

Κακόβουλο λογισμικό

Ένα κλικ μπορεί να αρκεί

Καθεμία διαφορετική. Όλες χειρότερες από το σπίτι.

Τι είναι το Phishing;

Το ψηφιακό ψάρεμα ευαίσθητων στοιχείων.

Απάτη που σας πείθει να δώσετε εθελοντικά κάτι πολύτιμο: κωδικό, στοιχείο ή πρόσβαση.

ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ ΜΗΧΑΝΙΚΑ:

1 ΠΡΟΣΕΛΚΥΕΙ
Ο επιτιθέμενος σας προσεγγίζει με ένα μήνυμα (email, SMS, κλήση, μήνυμα κ.λπ.).

→

2 ΠΡΟΣΠΟΙΕΙΤΑΙ
Παριστάνει μια αξιόπιστη οντότητα (π.χ. τράπεζα, εταιρεία, συνεργάτη, υπηρεσία).

→

3 ΠΑΡΑΠΛΑΝΕΙ
Δημιουργεί επείγουσα ανάγκη ή κίνητρο για να σας παρασύρει να ενεργήσετε.

→

4 ΣΑΣ ΟΔΗΓΕΙ
Σας οδηγεί σε έναν ψεύτικο σύνδεσμο ή σελίδα που μοιάζει αληθινή.

→

5 ΑΠΟΣΠΑ
Σας πείθει να δώσετε τα στοιχεία σας ή να παραχωρήσετε πρόσβαση.

Αποτέλεσμα: Ο επιτιθέμενος αποκτά **πρόσβαση** στους λογαριασμούς σας, στα δεδομένα σας ή στην εταιρεία σας.

91% ΤΩΝ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΞΕΚΙΝΟΥΝ ΑΠΟ ΑΝΘΡΩΠΙΝΟ ΛΑΘΟΣ

ΜΕΣΩ ΕΠΙΘΕΣΕΩΝ PHISHING

Re

W

Τράπεζα Κύπρου <w3743614538144_ftp_9696c49995b28847bacf3ccc0212...

Today at 12:04 PM

To: george@axis.ac.cy

Τράπεζα Κύπρου

Αγαπητέ Πελάτη ,

Προκειμένου να σας παρέχουμε την καλύτερη δυνατή εξυπηρέτηση, οι πληροφορίες σας πρέπει να είναι πάντα ακριβείς και να ενημερώνονται τακτικά.

Παρατηρήσαμε ότι τα δεδομένα σας για το 2023/2024 θα είναι σύντομα ξεπερασμένα στο σύστημά μας. Ως εκ τούτου, σας ζητάμε να μας βοηθήσετε να ενημερώσουμε τα στοιχεία σας,

Ενημέρωση τώρα

* Ορισμένες λειτουργίες του λογαριασμού σας δεν είναι προσωρινά διαθέσιμες μέχρι να ενημερωθούν τα δεδομένα σας.

Σας ευχαριστούμε για τη συνεργασία σας ,

© 2010-2025 Τράπεζα Κύπρου

Support <support@msupdate.net>
to me

4:09 PM (26 minutes ago)

Microsoft account

Your password changed

Your password for the Microsoft account ethan@hooksecurity.co was changed.

If this was you, then you can safely ignore this email.

Security info used:

Country/region: United States
Platform: iOS

Browser: Safari

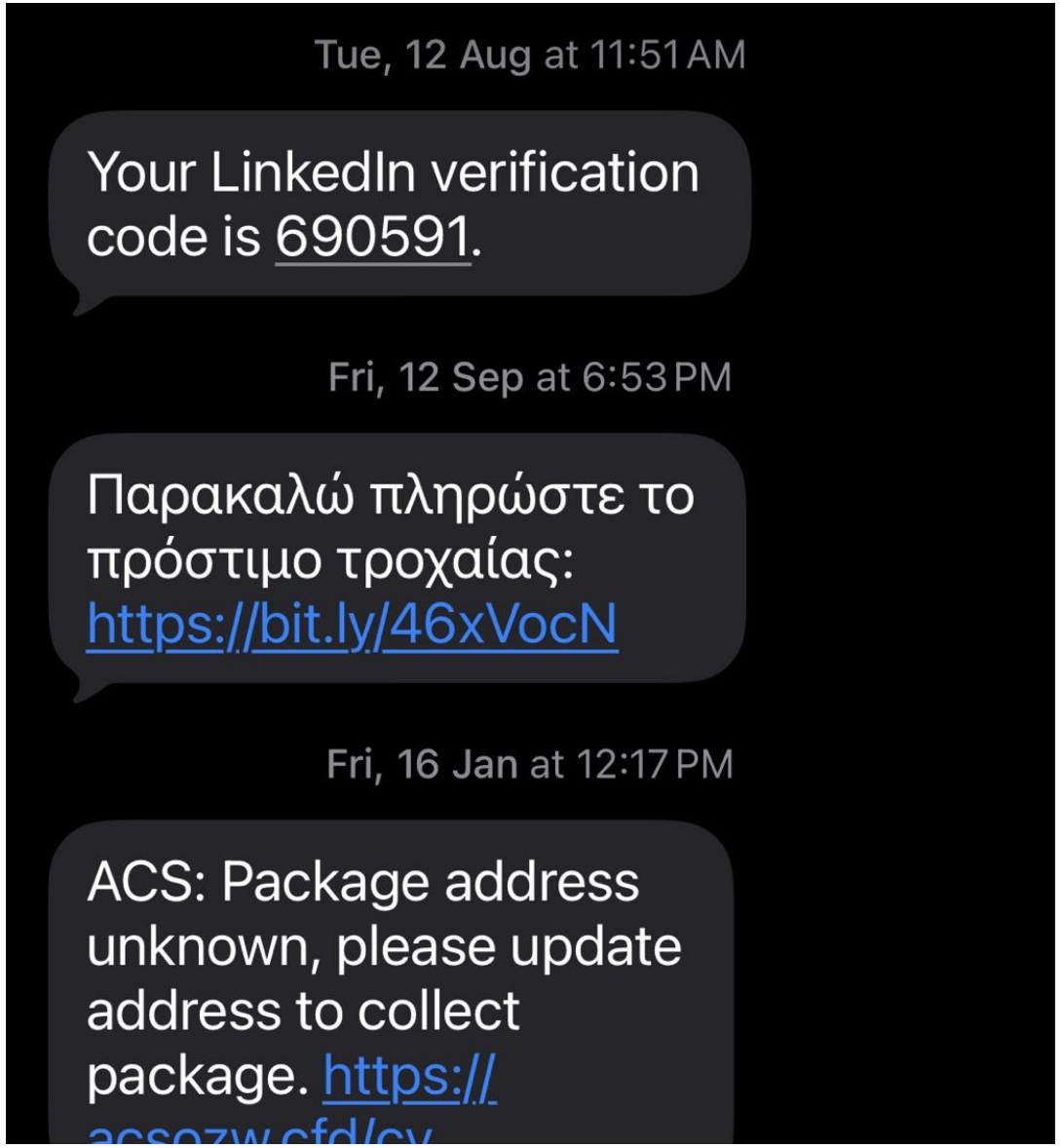
IP address: 77.196.86.10

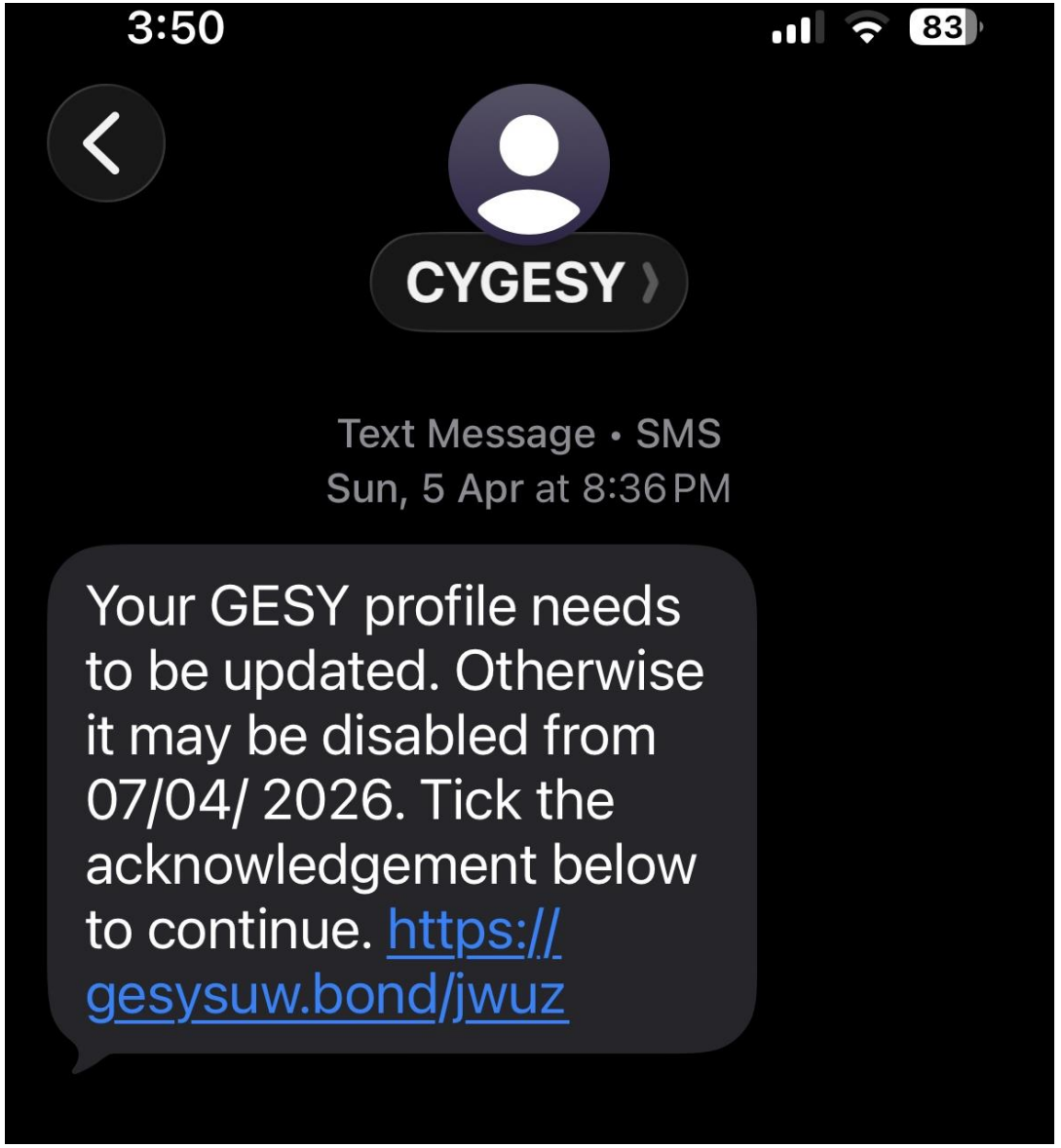
If this wasn't you, your account has been compromised. Please follow these steps:

1. Reset your password.
2. Review your security info.
3. Learn how to make your account more secure.

You can also opt out or change where you receive security notifications.

Thanks,


Tue, 12 Aug at 11:51 AM
Your LinkedIn verification code is 690591.
Fri, 12 Sep at 6:53 PM
Παρακαλώ πληρώστε το πρόστιμο τροχαίας: https://bit.ly/46xVocN
Fri, 16 Jan at 12:17 PM
ACS: Package address unknown, please update address to collect package. https://


3:50
83
CYGESY
Text Message • SMS
Sun, 5 Apr at 8:36 PM
Your GESY profile needs to be updated. Otherwise it may be disabled from 07/04/ 2026. Tick the acknowledgement below to continue. https://gesysuw.bond/jwuz

ΑΔΥΝΑΜΟΣ ΚΩΔΙΚΟΣ

Kypros20!

- Μικρό μήκος
- Κοινή λέξη
- Προβλέψιμο μοτίβο

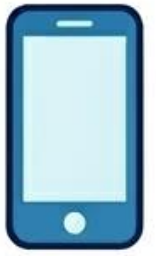
ΔΥΝΑΤΗ ΦΡΑΣΗ ΠΡΟΣΒΑΣΗΣ

KafePinoStonIlio2026!@

- Μεγάλο μήκος
- Τυχαίο
- Δύσκολο να μαντευτεί

1. Μοναδικότητα
Χρησιμοποιήστε μοναδικό κωδικό για κάθε λογαριασμό.

2. Password Manager
Χρησιμοποιήστε εργαλεία διαχείρισης κωδικών.



Απειλή 3: Όταν η προσωπική συσκευή γίνεται εταιρική απειλή.

Το laptop του σπιτιού δεν είναι ποτέ μόνο "του σπιτιού".

Α. ΤΡΕΙΣ ΤΡΟΠΟΙ ΜΕ ΤΟΥΣ ΟΠΟΙΟΥΣ ΕΙΣΕΡΧΕΤΑΙ ΤΟ MALWARE ΜΕΣΩ ΠΡΟΣΩΠΙΚΩΝ ΣΥΣΚΕΥΩΝ

1. Phishing & Ψευδή Links

Ένα κλικ αρκεί για να ανοίξει η πόρτα.

2. Μολυσμένα Downloads

Κατεβάζεις κάτι χρήσιμο, παίρνεις κάτι επικίνδυνο.

3. Μολυσμένα USB & Συσκευές

Ένα μικρό USB μπορεί να φέρει μεγάλο κακό.

Β. ΤΟ ΑΠΟΤΕΛΕΣΜΑ: RANSOMWARE

Το malware κρυπτογραφεί τα αρχεία σου, σταματά την εργασία σου, ζητά λύτρα.

Η ΜΟΝΗ ΠΡΑΓΜΑΤΙΚΗ ΑΜΥΝΑ: ΤΟ BACKUP.

Αν έχεις καθαρό backup, έχεις επιλογές.
Αν δεν έχεις, δεν έχεις τίποτα.

Πώς το AI άλλαζε το παιχνίδι

Οι κανόνες άμυνας του χθες δεν λειτουργούν αύριο

ΧΘΕΣ

Phishing με ορθογραφικά λάθη

Αγαπητέ πελάτι, λογαριαζμός σας...

Εύκολο να ξεχωρίσει.
Γενικά μηνύματα.
"Αγαπητέ Πελάτη".

ΣΗΜΕΡΑ

Εξατομικευμένο Phishing (Spear Phishing)

Αγαπητέ [Όνομα], παρακαλούμε επιβακαλούμε επβαιώστε την πληρωμή...

Τέλειος γραμματικός λόγος.
Στόχευση με όνομα/ρόλο.
Δύσκολο να αναγνωριστεί.

ΑΥΡΙΟ

Deepfake & AI Phishing

Αληθοφανή βίντεο/φωνή. "Ο CEO σου ζητάει..."

Αυτοματοποιημένες επιθέσεις.
Χρήση Deepfakes (φωνή/βίντεο).
Αδύνατο να ξεχωρίσει από την πραγματικότητα.

Ο κανόνας: ΣΤΑΜΑΤΑ — ΣΚΕΨΟΥ — ΕΛΕΓΞΕ

Τρία βήματα πριν αντιδράσετε σε οποιοδήποτε ύποπτο μήνυμα.

1 ΣΤΑΜΑΤΑ

Μην αντιδράσεις.
Κάνε παύση.

2 ΣΚΕΨΟΥ

Σκέψου κριτικά.
Κάτι δεν πάει καλά;

3 ΕΛΕΓΞΕ

Επαλήθευσε από επίσημη πηγή.
Όταν έχεις αμφιβολία, έλεγξε.

Ισχύει για κάθε κανάλι: email, τηλέφωνο, SMS, WhatsApp, βιντεοκλήση

Το σχέδιο δράσης σας

Συγκεκριμένα βήματα για την τηλεργασία — από Δευτέρα πρωί

Για τους τηλεργαζόμενους

1. **Ασφαλές οικιακό Wi-Fi**
   Αλλαγή προεπιλεγμένου κωδικού router, WPA3, ξεχωριστό δίκτυο για guests
2. **Ξεχωριστός λογαριασμός χρήστη για τη δουλειά**
   Όχι admin, όχι κοινός με την οικογένεια — δικός σας, με δικό σας κωδικό
3. **Επιβεβαίωση φωνής/βίντεο μέσω άλλου καναλιού**
   Εάν ζητηθεί "ευαίσθητη" ενέργεια, καλέστε τον αιτούντα στο τηλέφωνο
4. **Ενημερωμένα συστήματα**
   Windows/macOS updates, antivirus, browser plugins — πάντα the latest
5. **Χρήση VPN**
   Συνδεθείτε ΠΑΝΤΑ στο εταιρικό VPN πριν ανοίξετε email ή αρχεία δουλειάς

Για τους διαχειριστές IT

1. **MFA (Multi-Factor Authentication) παντού**
   Επιβολή MFA σε VPN, email, SaaS εφαρμογές — χωρίς εξαιρέσεις
2. **Εκπαίδευση & "Phishing Simulations"**
   Συχνές δοκιμές, άμεσο feedback στους χρήστες, βίντεο ευαισθητοποίησης
3. **Σαφείς πολιτικές ασφάλειας**
   Πώς διακινούνται αρχεία, πού αποθηκεύονται, πώς αναφέρεται ένα περιστατικό
4. **Έλεγχος των "Σκιωδών IT" (Shadow IT)**
   Μπλοκάρετε μη εγκεκριμένα cloud storage, messaging apps σε εταιρικές συσκευές
5. **Παρακολούθηση (Monitoring) logs**
   Έλεγχος για ασυνήθιστα logins (π.χ. από άγνωστες χώρες, περίεργες ώρες)

Η τηλεργασία δεν είναι λιγότερο ασφαλής.

Είναι διαφορετικά ασφαλής.

Κάθε τηλεργαζόμενος είναι είτε σημείο εισόδου,
είτε πρώτη γραμμή άμυνας. Η διαφορά είναι η εκπαίδευση.

Ας συνεχίσουμε τη συζήτηση

george@axis.ac.cy

77 788 748

www.axis.ac.cy