Deepfakes: Η νέα απειλή στην Κυβερνοασφάλεια

Αναγνώριση και αντιμετώπιση για επιχειρήσεις — Ενημέρωση και προστασία των εργαζομένων στη σύγχρονη ψηφιακή εποχή.

Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry

safeLine.gr

ΙΤΕ
ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Τι είναι τα Deepfakes;

Τα deepfakes είναι συνθετικό ψηφιακό περιεχόμενο που δημιουργείται με τη βοήθεια Τεχνητής Νοημοσύνης (AI). Μπορούν να απεικονίσουν πραγματικά πρόσωπα να λένε ή να κάνουν πράγματα που ποτέ δεν έγιναν, με εντυπωσιακή ρεαλιστικότητα.

Ψεύτικες εικόνες

Φωτογραφίες προσώπων που δεν υπάρχουν ή παραποιημένες εικόνες πραγματικών ατόμων.

Ψεύτικα βίντεο

Βίντεο με αντικατάσταση προσώπου ή ολόκληρης της εμφάνισης ενός ατόμου.

Ψεύτικες φωνές

Κλωνοποίηση φωνής για την προσομοίωση ομιλίας οποιουδήποτε ατόμου.

Συνθετικό περιεχόμενο

Πλήρως τεχνητά δημιουργημένα πρόσωπα, σκηνές και διαλόγους από AI.

Γιατί αποτελούν απειλή για τις επιχειρήσεις;

Οι κυβερνοεγκληματίες αξιοποιούν τα deepfakes για να παραπλανήσουν εργαζόμενους, να αποσπάσουν χρήματα ή εμπιστευτικές πληροφορίες. Η απειλή είναι άμεση και συνεχώς αυξανόμενη.

Ψεύτικοι διευθυντές

Προσομοίωση CEO ή ανώτατων στελεχών για έγκριση παράνομων συναλλαγών.

Ψεύτικοι πελάτες

Παραπλάνηση υπαλλήλων μέσω ψεύτικων ταυτοτήτων πελατών.

Ψεύτικες τηλεδιασκέψεις

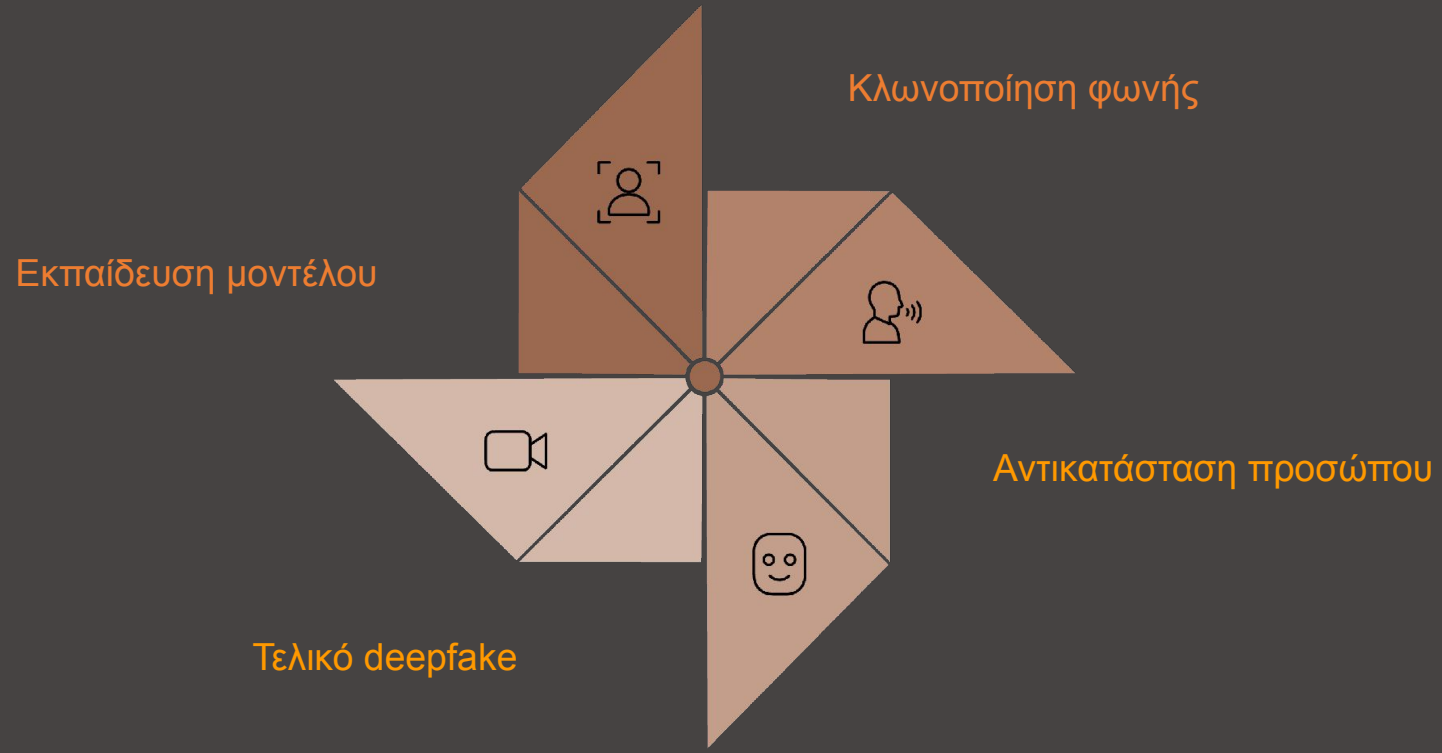
Ψεύτικες video κλήσεις με παραποιημένη εμφάνιση εμπίστων προσώπων.

Ψεύτικες κλήσεις

Κλωνοποιημένη φωνή προϊσταμένου για άμεσες εντολές μεταφοράς κεφαλαίων.

Πώς δημιουργούνται τα deepfakes;

Η διαδικασία δημιουργίας ενός deepfake δεν απαιτεί πλέον εξειδικευμένες γνώσεις. Σύγχρονα εργαλεία AI καθιστούν τη δημιουργία τους προσιτή σε σχεδόν οποιονδήποτε εντός λίγων λεπτών.



Το αποτέλεσμα είναι συνθετικό περιεχόμενο που μπορεί να είναι εξαιρετικά πειστικό — ακόμα και για εκπαιδευμένο μάτι. Η κατανόηση αυτής της διαδικασίας βοηθά στην αναγνώρισή τους.

Κατηγορίες επιθέσεων με deepfakes

Τα deepfakes χρησιμοποιούνται σε συγκεκριμένους τύπους κυβερνοεπιθέσεων που στοχεύουν εταιρείες. Η γνώση των τύπων αυτών είναι το πρώτο βήμα προστασίας.

1

CEO fraud

Ο επιτιθέμενος προσποιείται τον CEO ή ανώτατο στέλεχος και ζητά άμεση μεταφορά χρημάτων ή εμπιστευτικών δεδομένων.

2

Business Email Compromise (BEC)

Συνδυασμός deepfake φωνής ή βίντεο με παραπλανητικά email για πλήρη πλαστοπροσωπία εταιρικής ταυτότητας.

3

Voice phishing (Vishing)

Κλήσεις με κλωνοποιημένη φωνή γνωστού προσώπου για απόσπαση κωδικών ή χρηματικών εντολών.

4

Fake video calls

Ψεύτικες τηλεδιασκέψεις όπου ο επιτιθέμενος εμφανίζεται ως αξιόπιστος συνεργάτης ή πελάτης.

Deepfake φωνής — Πώς λειτουργεί

Ο επιτιθέμενος αναλύει δείγματα φωνής από δημόσιες πηγές (συνεντεύξεις, βίντεο) και δημιουργεί ένα πειστικό αντίγραφο σε λίγα μόνο λεπτά. Στη συνέχεια καλεί έναν υπάλληλο, προσποιούμενος τον διευθυντή.

> *"Είμαι ο Διευθυντής. Χρειάζομαι άμεση μεταφορά €50.000 σε νέο λογαριασμό. Είναι επείγον."*

Αυτές οι κλήσεις δημιουργούν αίσθηση επείγοντος για να αποτρέψουν κάθε επαλήθευση.

Πώς αντιδράμε;

→ **Μείνετε ψύχραιμοι**

Η επείγουσα γλώσσα είναι κόκκινη σημαία. Σταματήστε πριν δράσετε.

→ **Κλείστε και επαληθεύστε**

Τερματίστε την κλήση και επικοινωνήστε μέσω γνωστού αριθμού.

→ **Ακολουθήστε τις διαδικασίες**

Καμία χρηματική εντολή δεν εκτελείται χωρίς έγγραφη επιβεβαίωση.

Deepfake video — Ψεύτικες τηλεδιασκέψεις

Οι ψεύτικες τηλεδιασκέψεις αποτελούν μια από τις πιο επικίνδυνες μορφές deepfake επίθεσης, καθώς εκμεταλλεύονται την εμπιστοσύνη που δημιουργεί η οπτική επαφή. Ο επιτιθέμενος μπορεί να προσομοιώσει συναδέλφους, πελάτες ή συνεργάτες.

Ελέγξτε την εικόνα

Παρατηρήστε αφύσικες κινήσεις, ασυγχρονισμό χειλιών και παράξενο φωτισμό στο πρόσωπο.

Ελέγξτε το φόντο

Ασυνέπειες στο περιβάλλον, θολές άκρες γύρω από το πρόσωπο ή παράξενη ποιότητα εικόνας.

Ζητήστε επαλήθευση

Ζητήστε από τον συνομιλητή να κάνει κάτι απρόβλεπτο — π.χ. να στρέψει το κεφάλι απότομα.

Επιβεβαιώστε εκτός κλήσης

Για σημαντικές αποφάσεις, επικοινωνήστε ξανά μέσω διαφορετικού καναλιού πριν προχωρήσετε.

Πώς αναγνωρίζουμε τα deepfakes;

Παρόλο που τα σύγχρονα deepfakes γίνονται όλο και πιο ρεαλιστικά, εξακολουθούν να αφήνουν χαρακτηριστικά ίχνη. Η εκπαίδευση στην αναγνώριση αυτών των σημαδιών είναι κρίσιμη για κάθε εργαζόμενο.

Αφύσικες κινήσεις προσώπου

Τα deepfakes συχνά παρουσιάζουν ασυνήθιστες ή μηχανικές εκφράσεις, ιδιαίτερα γύρω από τα μάτια και το στόμα.

Ασυγχρονία χειλιών και παράξενη φωνή

Η κίνηση των χειλιών δεν συμβαδίζει απόλυτα με τον ήχο. Η φωνή μπορεί να ακούγεται επίπεδη ή μηχανική.

Αφύσικος φωτισμός και ασυνέπειες

Ο φωτισμός στο πρόσωπο δεν ταιριάζει με το περιβάλλον. Το φόντο μπορεί να έχει θολές ή παράξενες άκρες.

Κανόνες επαλήθευσης — Η πρώτη γραμμή άμυνας

❌ Ποτέ μην βασίζεστε μόνο σε:

- **Φωνή:** Ακόμα και η πιο οικεία φωνή μπορεί να κλωνοποιηθεί.
- **Βίντεο:** Η οπτική επαφή δεν εγγυάται αυθεντικότητα.
- **Εικόνα:** Φωτογραφίες και screenshots παραποιούνται εύκολα.

✅ Επαληθεύστε πάντα μέσω:

→ **Δεύτερου καναλιού επικοινωνίας**

Επικοινωνήστε μέσω διαφορετικής πλατφόρμας από αυτήν που λάβατε το αίτημα.

→ **Γνωστού τηλεφώνου**

Χρησιμοποιήστε τον αριθμό που έχετε ήδη αποθηκευμένο, όχι αυτόν που σας δίνεται.

→ **Εταιρικής διαδικασίας**

Ακολουθήστε πιστά τις εγκεκριμένες διαδικασίες εταιρείας για εντολές υψηλής αξίας.

Μέτρα προστασίας για επιχειρήσεις

Η αποτελεσματική άμυνα απέναντι στα deepfakes απαιτεί συνδυασμό τεχνολογικών εργαλείων και ανθρώπινης επαγρύπνησης. Κανένα μεμονωμένο μέτρο δεν αρκεί από μόνο του.

MFA — Πολλαπλή ταυτοποίηση

Η χρήση δεύτερου παράγοντα αυθεντικοποίησης προστατεύει ακόμα και αν κλαπούν κωδικοί.

Διαδικασίες επαλήθευσης

Τυποποιημένες διαδικασίες για κάθε χρηματική εντολή ή μεταφορά εμπιστευτικών πληροφοριών.

Four eyes principle

Κάθε κρίσιμη ενέργεια εγκρίνεται από δύο διαφορετικά άτομα για αποφυγή μονομερών λαθών.

Security awareness

Τακτική εκπαίδευση εργαζομένων στις νέες τακτικές επίθεσης και στην αναγνώριση απειλών.

Password managers & Least privilege

Χρήση διαχειριστή κωδικών και αρχή ελάχιστων δικαιωμάτων για περιορισμό έκθεσης.

Καλή vs κακή πρακτική

Η διαφορά μεταξύ ασφάλειας και παραβίασης συχνά εξαρτάται από μια απλή απόφαση: επαλήθευση ή άμεση συμμόρφωση;

🟢 Καλή πρακτική

Ο υπάλληλος λαμβάνει τηλεφωνική εντολή από τον «Διευθυντή» για μεταφορά χρημάτων.

- Δεν εκτελεί αμέσως.
- Κλείνει την κλήση.
- Καλεί τον Διευθυντή στον γνωστό αριθμό.
- Επιβεβαιώνει και μόνο τότε ενεργεί.

✓ Αποτέλεσμα: Η επίθεση αποτρέπεται.

🔴 Κακή πρακτική

Ο υπάλληλος λαμβάνει την ίδια εντολή.

- Αναγνωρίζει τη φωνή του διευθυντή.
- Εμπιστεύεται χωρίς αμφιβολία.
- Εκτελεί άμεσα τη μεταφορά.
- Ανακαλύπτει αργότερα ότι ήταν deepfake.

✗ Αποτέλεσμα: Σημαντική χρηματική ζημιά για την εταιρεία.

Checklist ασφάλειας για κάθε εργαζόμενο

Τηρείτε αυτές τις πέντε βασικές αρχές καθημερινά για να προστατέψετε εσάς και την εταιρεία σας από επιθέσεις με deepfakes.

Επιβεβαίωση ταυτότητας

Πάντα επαληθεύετε ποιος σας μιλά μέσω δεύτερου, ανεξάρτητου καναλιού επικοινωνίας — ειδικά για επείγοντα αιτήματα.

Τήρηση εταιρικών διαδικασιών

Καμία εξαίρεση στις εγκεκριμένες διαδικασίες, ανεξαρτήτως του πόσο επείγον φαίνεται το αίτημα.

Χρήση MFA

Ενεργοποιήστε τον δεύτερο παράγοντα ταυτοποίησης σε όλα τα εταιρικά συστήματα και εφαρμογές.

Αναφορά ύποπτων περιστατικών

Αναφέρετε άμεσα κάθε ύποπτη επικοινωνία στο IT/Security τμήμα — ακόμα και αν δεν είστε σίγουροι.

Συνεχής εκπαίδευση & ενημέρωση

Συμμετέχετε σε τακτικές εκπαιδεύσεις ευαισθητοποίησης για τις νέες τεχνικές κυβερνοεπιθέσεων.

Συμπεράσματα

Τα deepfakes εξελίσσονται ραγδαία και θα γίνονται όλο και πιο πειστικά. Η τεχνολογία από μόνη της δεν είναι αρκετή για την αντιμετώπισή τους.

🧠 Ενημέρωση

Γνωρίστε τις τακτικές των επιτιθέμενων για να τις αναγνωρίζετε εγκαίρως.

📋 Διαδικασίες

Εφαρμόστε αυστηρές διαδικασίες επαλήθευσης για κάθε κρίσιμη εντολή.

👥 Εκπαίδευση

Ο καλύτερα εκπαιδευμένος εργαζόμενος είναι η πιο αποτελεσματική άμυνα.

Θυμηθείτε: Μια στιγμή επαλήθευσης μπορεί να σώσει την εταιρεία από σημαντική ζημιά.