Τι είναι η Κυβερνοασφάλεια;

Η κυβερνοασφάλεια αποτελεί το σύνολο των πρακτικών, τεχνολογιών και διαδικασιών που σχεδιάζονται για την προστασία υπολογιστών, δικτύων, προγραμμάτων και δεδομένων από επιθέσεις, ζημιές ή μη εξουσιοδοτημένη πρόσβαση στο διαδίκτυο.

Στη σύγχρονη ψηφιακή εποχή, η κυβερνοασφάλεια είναι απαραίτητη για την προστασία της ιδιωτικότητας, της επιχειρηματικής συνέχειας και της εθνικής ασφάλειας.

Απειλές και Κυβερνοασφάλεια

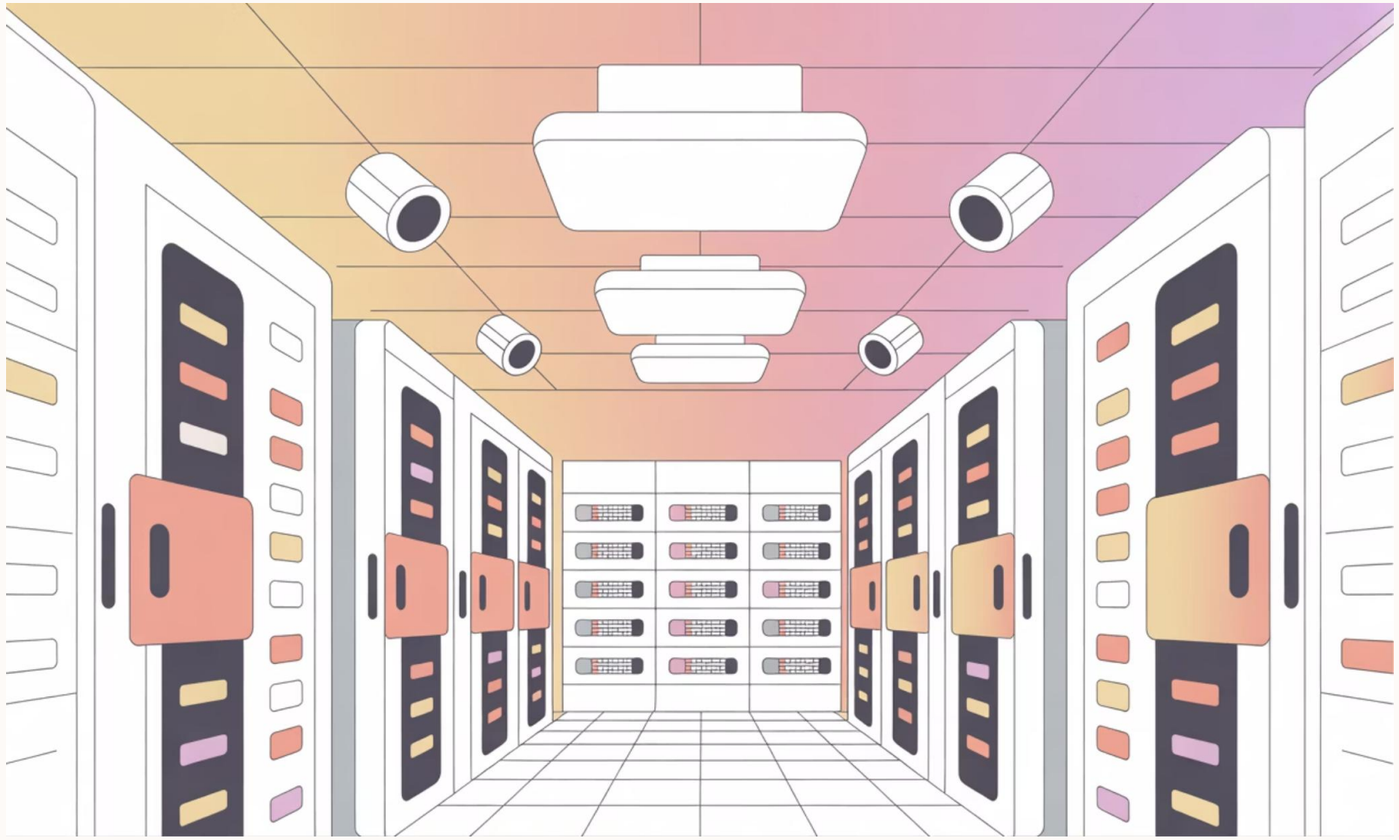
Τι είναι Απειλή;

Με τον όρο απειλή περιγράφουμε οποιοδήποτε γεγονός που δύναται να επιφέρει μερική ή ολική αλλοίωση των ψηφιακών αγαθών και πληροφοριών.

Είδη Απειλών

Οι απειλές μπορεί να συμβούν με φυσικό τρόπο (πρόσβαση σε εξοπλισμό) ή με ηλεκτρονικό τρόπο (κυβερνοεπιθέσεις, malware, hacking).

Φυσική Ασφάλεια



Προστασία Υποδομών

Τα data centers και οι προσωπικοί υπολογιστές πρέπει να προστατεύονται από τη φυσική πρόσβαση μη εξουσιοδοτημένων χρηστών με συστήματα ελέγχου πρόσβασης, κάμερες και κλειδαριές.

Φυσικοί Κίνδυνοι

Επίσης, πρέπει να προστατεύονται από φυσικούς κινδύνους όπως φωτιά, πλημμύρες και σεισμούς με συστήματα πυρόσβεσης, γεννήτριες και εφεδρικά συστήματα.

Σύγχρονος Τρόπος Ζωής και Απειλές

Κοινωνικά Δίκτυα

Καθημερινή χρήση πλατφορμών όπως Facebook, Instagram και Twitter που αποθηκεύουν προσωπικές πληροφορίες.

Ηλεκτρονικές Πληρωμές

Online αγορές και συναλλαγές με κάρτες που απαιτούν προστασία οικονομικών δεδομένων.

Τραπεζικές Συναλλαγές

Ψηφιακή τραπεζική που εκθέτει λογαριασμούς σε κυβερνοκινδύνους.

Κακόβουλοι Χρήστες

Hackers που προσπαθούν να αποκτήσουν παράνομη πρόσβαση σε δεδομένα, κωδικούς και προσωπικές πληροφορίες.

ΚΕΦΆΛΑΙΟ 6.3

Επίπεδα Ασφάλειας και Εφαρμογή τους

Επίπεδο Υπολογιστή

Προστασία μεμονωμένων συσκευών και λειτουργικών συστημάτων

Επίπεδο Δικτύου

Ασφάλεια δικτυακών υποδομών και επικοινωνιών

Πληροφοριακά Συστήματα

Προστασία cloud υπηρεσιών και IoT συσκευών

Η ολοκληρωμένη ασφάλεια απαιτεί συντονισμένη προστασία σε όλα τα επίπεδα, από τον ατομικό υπολογιστή μέχρι τα σύννεφα και το Διαδίκτυο των Πραγμάτων.

ΚΕΦΆΛΑΙΟ 6.3.1

Ασφάλεια σε Επίπεδο Υπολογιστή

Κυβερνοαπειλές

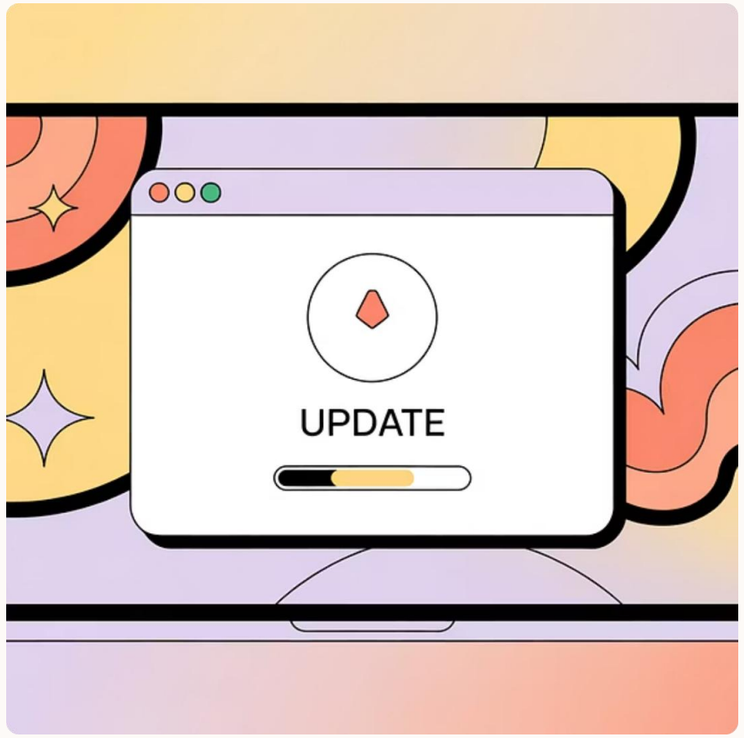
Ο υπολογιστής μπορεί να μολυνθεί από διάφορες μορφές κακόβουλου λογισμικού:

- **Ιοί:** Προγράμματα που αναπαράγονται και μολύνουν αρχεία
- **Σκουλήκια:** Αυτοδιαδιδόμενα προγράμματα που εξαπλώνονται σε δίκτυα
- **Δούρειοι Ίπποι:** Κρυμμένο κακόβουλο λογισμικό σε φαινομενικά ασφαλή προγράμματα
- **Ransomware:** Κρυπτογράφηση αρχείων με απαίτηση λύτρων
- **Malvertising:** Κακόβουλες διαφημίσεις στο διαδίκτυο
- **Phishing:** Απάτη μέσω email και ψεύτικων ιστοσελίδων

Προσοχή!

Κίνδυνο συνιστούν και οι μολυσμένες συσκευές USB που μπορούν να μεταδώσουν malware απευθείας στον υπολογιστή σας.

Ενημερώσεις και Antivirus



Ενημερώσεις Συστήματος

Ο χρήστης πρέπει να έχει ενεργοποιημένες τις αυτόματες ενημερώσεις του λειτουργικού συστήματος για να λαμβάνει διορθώσεις ασφαλείας και patches.

Αντιϊικό Λογισμικό

Πρέπει να έχει εγκατεστημένο και ενημερωμένο Αντιϊικό Λογισμικό (antivirus) που σαρώνει και αφαιρεί κακόβουλο λογισμικό σε πραγματικό χρόνο.

Phishing και Κωδικοί

Προσοχή στα Email

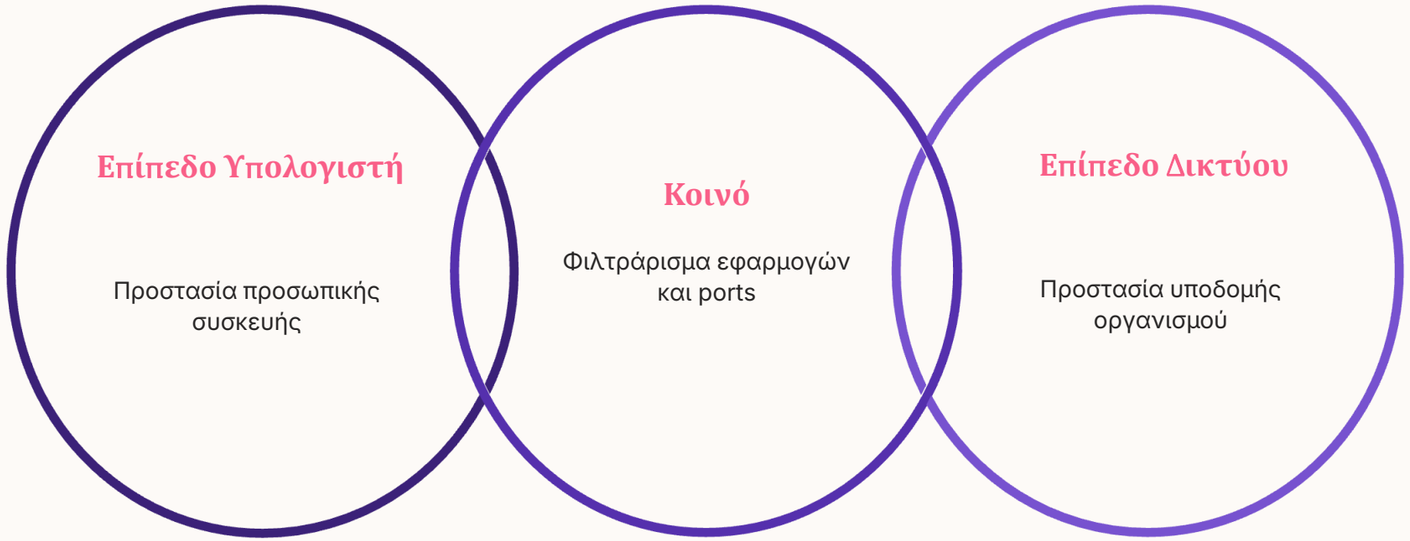
Κακόβουλα e-mail τύπου phishing προσπαθούν να μας ξεγελάσουν με ψεύτικες ιστοσελίδες τραπεζών, εταιρειών ή δημόσιων υπηρεσιών για να κλέψουν τα στοιχεία μας.

Μυστικότητα Κωδικών

Δε δίνουμε ποτέ και σε κανέναν τους κωδικούς μας. Καμία νόμιμη υπηρεσία δεν θα ζητήσει ποτέ τον κωδικό σας μέσω email ή τηλεφώνου.

Συμβουλή: Χρησιμοποιείτε μοναδικούς, ισχυρούς κωδικούς για κάθε υπηρεσία και ενεργοποιείτε την επαλήθευση δύο παραγόντων (2FA) όπου είναι διαθέσιμη.

Τείχος Προστασίας (Firewall)



Το firewall λειτουργεί σαν φρουρός που ελέγχει την εισερχόμενη και εξερχόμενη κίνηση δεδομένων.

Πώς Λειτουργεί

Το τείχος προστασίας εφαρμόζεται σε επίπεδο υπολογιστή (personal firewall) ή δικτύου (network firewall) και επιτρέπει πρόσβαση μόνο σε συγκεκριμένες υπηρεσίες και διευθύνσεις IP που θεωρούνται ασφαλείς.

Μπλοκάρει μη εξουσιοδοτημένες συνδέσεις και προστατεύει από κακόβουλες επιθέσεις.

Προστασία Προσωπικών Δεδομένων

Προσοχή στα Social Media

Δεν δίνουμε προσωπικά στοιχεία όπως διεύθυνση κατοικίας, αριθμούς τηλεφώνου, οικονομικές πληροφορίες ή φωτογραφίες ευαίσθητων εγγράφων στα Μέσα Κοινωνικής Δικτύωσης.

Μην Ανακοινώνετε Απουσίες

Δεν κοινοποιούμε ότι είμαστε σε διακοπές ή μακριά από το σπίτι, καθώς αυτό μπορεί να προσελκύσει κλέφτες και να θέσει σε κίνδυνο την ασφάλεια της κατοικίας μας.

Ρυθμίσεις Απορρήτου

Ελέγχετε τακτικά τις ρυθμίσεις απορρήτου στους λογαριασμούς σας και περιορίστε ποιος μπορεί να δει τις αναρτήσεις και τις πληροφορίες σας.

Κρυπτογραφία: Προστασία Δεδομένων στην Ψηφιακή Εποχή

Μάθετε πώς η κρυπτογράφηση διασφαλίζει την ασφάλεια των πληροφοριών σας στο διαδίκτυο και γιατί αποτελεί τη βάση της σύγχρονης κυβερνοασφάλειας.

Τι είναι η Κρυπτογράφηση;

Ορισμός

Η κρυπτογράφηση είναι η εφαρμογή τεχνικής για τη μετατροπή της πληροφορίας σε μορφή μη αναγνωρίσιμη, ώστε να μην μπορεί να διαβαστεί από μη εξουσιοδοτημένα άτομα κατά την αποθήκευση ή μεταφορά.

Αποκρυπτογράφηση

Η αντίστροφη διαδικασία που επιτρέπει σε εξουσιοδοτημένους χρήστες να ανακτήσουν την αρχική πληροφορία χρησιμοποιώντας το κατάλληλο κλειδί.

Βασικά Είδη Κρυπτογράφησης

Συμμετρική Κρυπτογράφηση

Χρησιμοποιεί ένα κοινό μυστικό κλειδί για κρυπτογράφηση και αποκρυπτογράφηση. Ο αποστολέας και ο παραλήπτης μοιράζονται το ίδιο κλειδί.

Ασύμμετρη Κρυπτογράφηση

Χρησιμοποιεί ζευγάρι κλειδιών: ένα δημόσιο για κρυπτογράφηση και ένα ιδιωτικό για αποκρυπτογράφηση. Μεγαλύτερη ασφάλεια χωρίς ανταλλαγή μυστικού.

Συμμετρική Κρυπτογράφηση: Ο Κώδικας του Καίσαρα

Τεχνική Ολίσθησης Αλφαβήτου

Η πιο γνωστή μορφή συμμετρικής κρυπτογράφησης. Κάθε γράμμα αντικαθίσταται από άλλο που βρίσκεται σε συγκεκριμένη απόσταση στο αλφάβητο.

Παράδειγμα με ολίσθηση 2

Αρχικό μήνυμα: ΚΑΛΗΜΕΡΑ

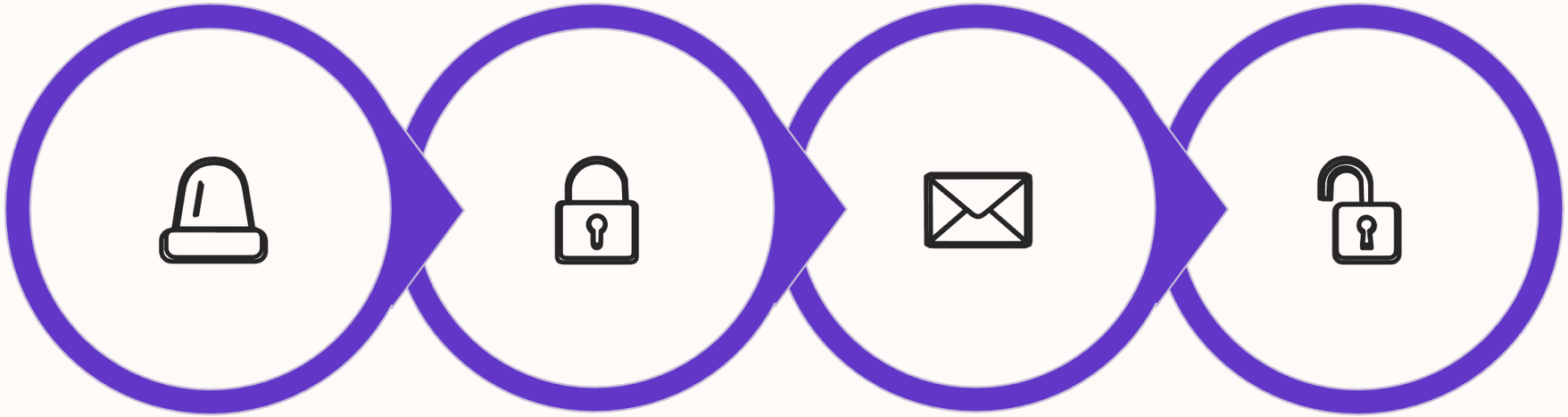
Κρυπτογραφημένο: ΜΓΝΙΞΗΤΓ

Κ→Μ, Α→Γ, Λ→Ν, Η→Ι, Μ→Ξ, Ε→Η, Ρ→Τ, Α→Γ

Το Μυστικό Κλειδί

Ο αριθμός θέσεων ολίσθησης (π.χ. 2, 3, 5) αποτελεί το κοινό μυστικό που πρέπει να γνωρίζουν αποστολέας και παραλήπτης.

Ασύμμετρη Κρυπτογράφηση: Δημόσιο & Ιδιωτικό Κλειδί



Στην ασύμμετρη κρυπτογράφηση χρησιμοποιούνται δύο συσχετισμένα κλειδιά. Το δημόσιο κλειδί μοιράζεται ελεύθερα, ενώ το ιδιωτικό παραμένει μυστικό. Αυτό που κρυπτογραφείται με το ένα, αποκρυπτογραφείται μόνο με το άλλο.

Πού Χρησιμοποιούμε Ασύμμετρη Κρυπτογράφηση;

HTTPS - Ασφαλείς Ιστοσελίδες

Όταν βλέπετε https αντί για http, η σύνδεσή σας προστατεύεται με κρυπτογράφηση δημοσίου κλειδιού.

Εικονικά Ιδιωτικά Δίκτυα (VPN)

Τα VPN χρησιμοποιούν ασύμμετρη κρυπτογράφηση για ασφαλή διασύνδεση σε δίκτυα.

Ψηφιακές Υπογραφές

Επικυρώνουν την ταυτότητα και την ακεραιότητα ηλεκτρονικών εγγράφων.

Κρυπτονομίσματα

Το Bitcoin και άλλα κρυπτονομίσματα βασίζονται σε αλγορίθμους όπως ο RSA.

Ψηφιακά Πιστοποιητικά & Αρχές Πιστοποίησης

Τι είναι η Αρχή Πιστοποίησης;

Επίσημος και ανεξάρτητος φορέας που επικυρώνει τη γνησιότητα των δημοσίων κλειδιών και πιστοποιεί την ταυτότητα των χρηστών.

Παραδείγματα στην Ελλάδα:

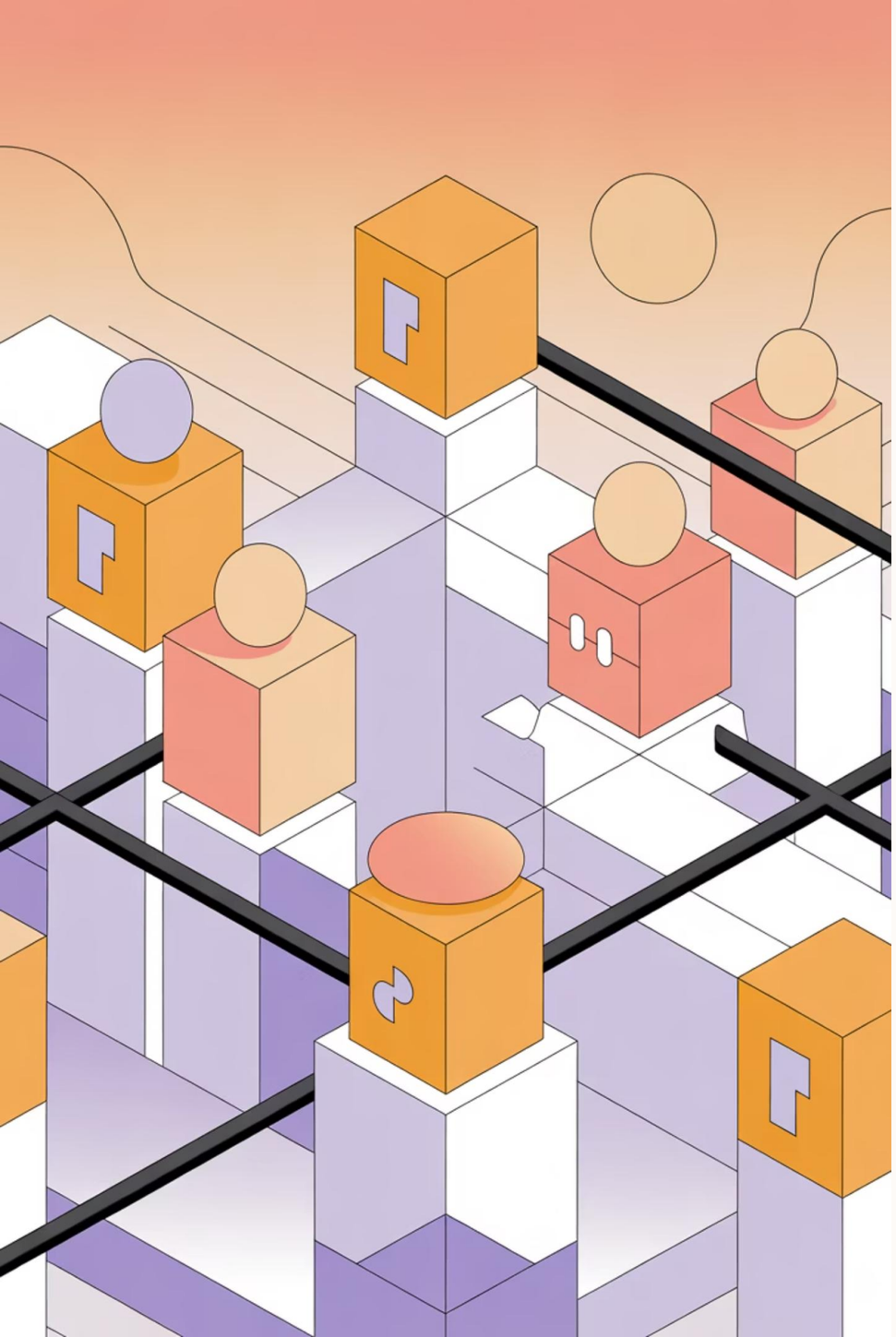
- Αρχή Πιστοποίησης Ελληνικού Δημοσίου
- Υπηρεσία ψηφιακών πιστοποιητικών του ΠΣΔ

Ψηφιακή Υπογραφή

Με έγκυρο ψηφιακό πιστοποιητικό, μπορείτε να υπογράφετε ηλεκτρονικά έγγραφα, εξασφαλίζοντας:

- **Αυθεντικότητα:** Επιβεβαίωση ταυτότητας υπογράφοντος
- **Ακεραιότητα:** Το έγγραφο δεν έχει τροποποιηθεί
- **Μη αποποίηση:** Αδυναμία άρνησης υπογραφής

Τα ηλεκτρονικά καταστήματα οφείλουν να διαθέτουν έγκυρα πιστοποιητικά για ασφαλείς συναλλαγές.



Τεχνολογία Blockchain: Αποκεντρωμένη Ασφάλεια

Πώς Λειτουργεί το Blockchain

Μια αλυσίδα από μπλοκ δεδομένων που αποθηκεύονται σε χιλιάδες υπολογιστές παγκοσμίως. Κάθε μπλοκ περιέχει συναλλαγές και το ψηφιακό αποτύπωμα (hash) του προηγούμενου.

Αποκεντρωμένο

Δεν ελέγχεται από κεντρική αρχή

Διαφανές

Όλες οι συναλλαγές είναι ορατές

Αμετάβλητο

Τα δεδομένα δεν μπορούν να αλλάξουν

Bitcoin: Η Πρώτη Εφαρμογή του Blockchain

Ψηφιακό Νόμισμα χωρίς Τράπεζες

Το Bitcoin είναι κρυπτονόμισμα που λειτουργεί μέσω αποκεντρωμένου δικτύου υπολογιστών. Χιλιάδες κόμβοι συντηρούν το Blockchain χωρίς διαμεσολαβητές.

Χαρακτηριστικά

- **Δημόσιες συναλλαγές:** Όλες καταγράφονται στο Blockchain
- **Διαφάνεια:** Ιχνηλασιμότητα κάθε συναλλαγής
- **Ψευδωνυμία:** Όχι πλήρης ιδιωτικότητα
- **Ακεραιότητα:** Αδύνατη η πλαστογράφηση

Βασικές Έννοιες για Επανάληψη

Κρυπτογράφηση

Μετατροπή πληροφορίας σε μη αναγνωρίσιμη μορφή για προστασία από μη εξουσιοδοτημένη πρόσβαση κατά την αποθήκευση ή μεταφορά.

Συμμετρική vs Ασύμμετρη

Η συμμετρική χρησιμοποιεί ένα κοινό κλειδί, η ασύμμετρη χρησιμοποιεί ζευγάρι δημοσίου-ιδιωτικού κλειδιού για μεγαλύτερη ασφάλεια.

Ψηφιακά Πιστοποιητικά

Επικυρώνουν τη γνησιότητα δημοσίων κλειδιών μέσω Αρχών Πιστοποίησης και επιτρέπουν ψηφιακές υπογραφές.

Blockchain

Αποκεντρωμένη τεχνολογία αποθήκευσης δεδομένων με διαφάνεια και αμεταβλητότητα. Βάση των κρυπτονομισμάτων όπως το Bitcoin.