

Password Safety



Why Passwords Matter



Passwords as Digital Keys

Passwords act as digital keys that safeguard sensitive personal and financial information from unauthorized access.

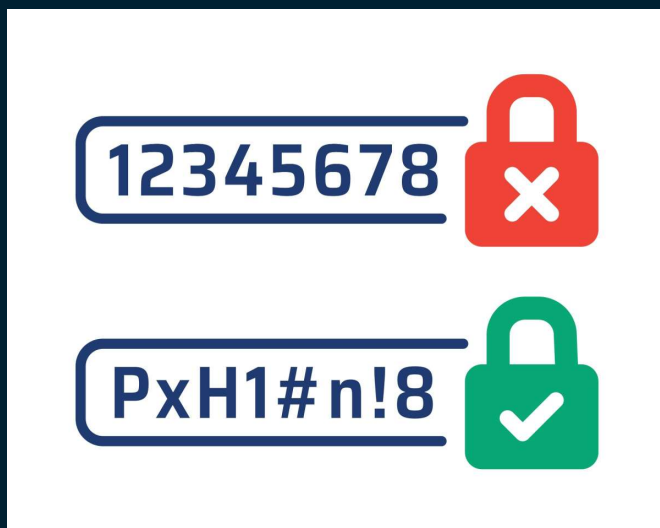
Risks of Weak Passwords

Weak or reused passwords are common vulnerabilities hackers exploit to gain unauthorized access to accounts.

Importance of Strong Passwords

Implementing strong, unique passwords is essential to reduce risks of identity theft and data breaches.

Creating Strong Passwords



Elements of Strong Passwords

Strong passwords include at least 12 characters with uppercase, lowercase, numbers, and symbols for complexity.

Avoid Predictable Patterns

Avoid real words, personal info, and common patterns like 'abc123' to enhance password security.

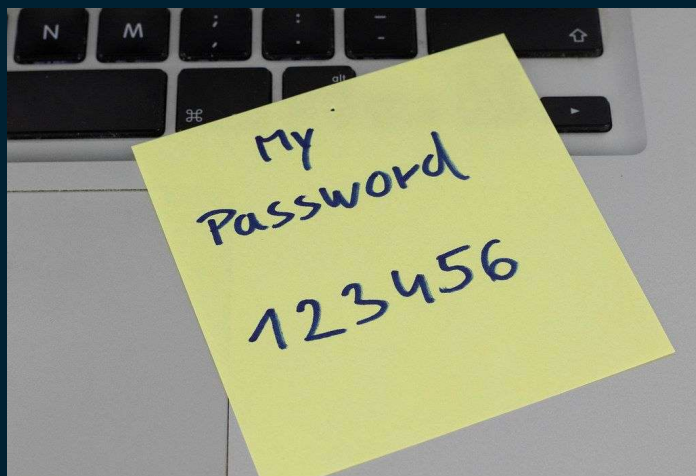
Using Passphrases

Use meaningful but random passphrases combining words, numbers, and symbols for strong passwords.

Randomness and Length Importance

Long and random passwords are harder to crack and provide stronger protection against attacks.

Avoiding Common Password Mistakes



Password Reuse Risk

Reusing passwords across accounts increases the risk of multiple account breaches from one compromised password.

Weak Passwords

Using simple or guessable passwords like '123456' makes accounts vulnerable to attacks.

Protect Password Privacy

Avoid sharing passwords or storing them insecurely to prevent unauthorized access.

Use Unique Passwords

Create unique passwords for each account, especially for important services like banking and email.

Secure Storage and Sharing Practices



Physical Password Storage

Store written passwords securely and discreetly, avoiding labels and never carrying them.

Digital Password Management

Use encrypted password managers with strong master passwords for digital security.

Avoid Password Sharing

Never share passwords; treat them like personal hygiene for security.

Phishing Awareness

Beware of phishing; always verify requests before sharing sensitive information.

Using Password Managers



Secure Password Storage

Password managers securely encrypt and store login credentials in a digital vault accessible via a master password.


Password Generation and Autofill

These tools generate complex passwords and automatically fill login details to enhance security and convenience.


Alternative Password Management

Writing passwords down and storing them securely at home is an alternative for those uneasy with digital storage.

Two-Factor Authentication (2FA)




Turn on 2-Step Verification
Open authenticator and choose scan barcode.




Continue

OR enter the code manually

LKS7 - 28HS - J910 - HAXX - 72LA - 0HAJ - SCBH





Verify Authentication Code
Enter the 6-digit code in authenticator.

3

7

1

-

|

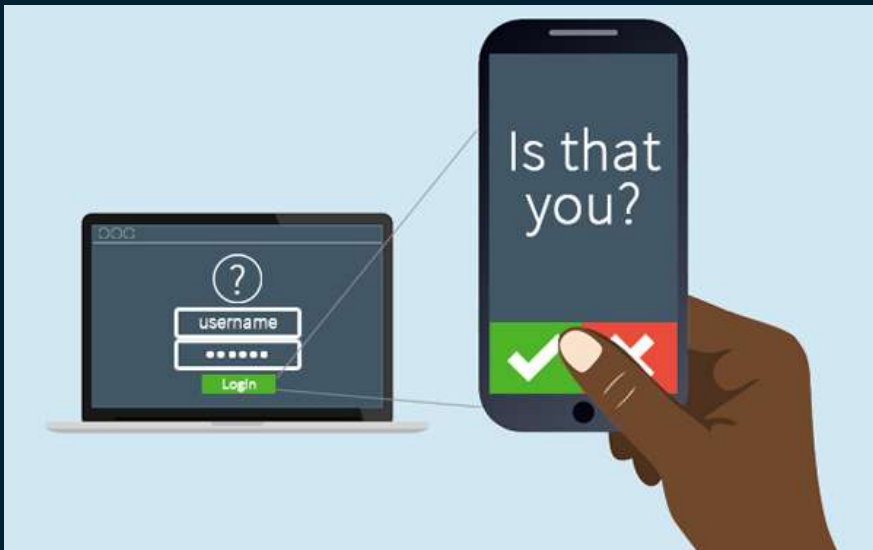
0

0

Complete 2-step verification

Having trouble? [Chat to our team](#)

Introduction to 2FA



Two Forms of Verification

2FA requires both something you know like a password and something you have like a verification code.

Common 2FA Methods

Popular 2FA methods include SMS codes, authenticator apps, and physical security tokens.

Effectiveness of MFA

Multi-Factor Authentication blocks over 99.9% of automated account attacks, enhancing online security.

Tips for Using 2FA



Enable 2FA on Critical Accounts

Activate two-factor authentication on email, banking, social media, and other sensitive accounts for maximum security.

Prefer Authenticator Apps Over SMS

Use authenticator apps instead of SMS codes as they provide stronger protection against interception.

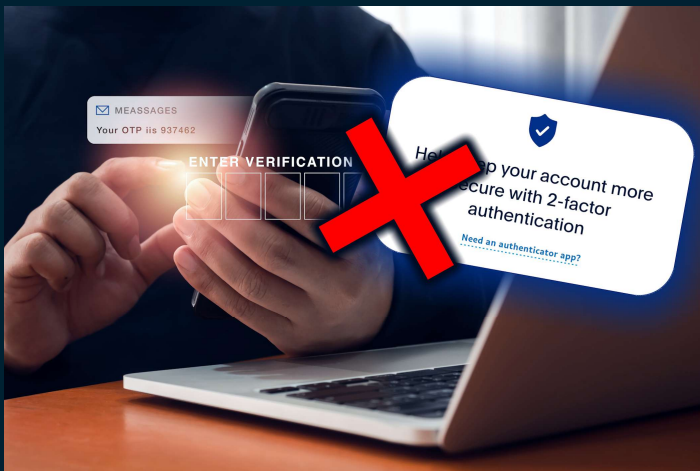
Save Backup Codes Securely

Store backup codes safely to maintain account access if your authentication device is lost or unavailable.

Trust Devices Temporarily

Leverage trusted device options to reduce login interruptions without compromising security.

Avoiding 2FA Scams



Understanding 2FA Scams

Scammers send unexpected 2FA codes and impersonate companies to trick you into revealing codes.

Never Share Your Codes

Always keep 2FA codes private and enter them only on the official login screens to stay safe.

Responding to Unrequested Codes

Receiving unrequested codes can indicate hacking attempts; change passwords and review security immediately.

Securing Your Devices



Device Access Protection

Use PINs, fingerprints, or facial recognition to prevent unauthorized device access and protect authentication apps.

App Source Caution

Avoid installing apps from untrusted sources to reduce the risk of malware compromising your device security.

Device as Digital Key

Treat your devices as a key to your digital life, safeguarding them to enhance Two-Factor Authentication effectiveness.

Updating and Monitoring Passwords

HACKER: 'I have all your passwords'
ME: 'OMG thank you! What are they?'



Importance of Password Updates

Regular updates protect against unauthorized access, especially after a suspected security breach.

Monitoring Breach Alerts

Use online tools to check if your credentials have been exposed in data breaches.

Prioritize Critical Accounts

Immediately update passwords for email, banking, and social media accounts to ensure safety.

Password & 2FA Checklist

Strong Unique Passwords

Use long, complex, and unique passwords for every account to enhance cybersecurity and prevent breaches.

Enable Two-Factor Authentication

Activate 2FA on important accounts like email, banking, and social media for an additional security layer.

Secure Password Storage

Store passwords safely in a trusted password manager or physical secure location to avoid unauthorized access.

Protect Your Verification Codes

Never share passwords or verification codes and keep your phone locked to protect the 2FA second factor.