

Everyday Cybersecurity

Practical protection for passwords, accounts, devices, and personal information.

WHAT YOU WILL LEARN

- Spot your highest-risk accounts and devices
- Build a strong password and recovery plan
- Set up multifactor authentication and reliable backups

4 lessons | 45-60 minutes | Free | Beginner

Course links and printable PDF: <https://blackcloudsecurity.org/learn/>

Important: conduct security tests only on your own systems or systems where you have explicit authorization. Use official training labs for guided practice.

LESSON 1 OF 4

Know what you need to protect

Cybersecurity begins with an inventory. You cannot defend an account you forgot exists. Start with the services that could affect money, identity, or your other accounts.

STEP-BY-STEP PRACTICE

1. Make a private list of five important accounts: primary email, banking, phone carrier, domain registrar, and cloud services are common examples. Never put passwords in the list.
2. For each account, note whether you can still access its recovery email and authenticator. Identify any that depend on an old phone number.
3. Write down which devices you use to sign in and whether each has a screen lock.
4. Pick one high-priority account to secure today. Start with your email because it may reset other passwords.

KEY TAKEAWAY

Your primary email and domain registrar often deserve the strongest protection.

CHECK YOUR KNOWLEDGE

Which account would usually be the highest priority to secure first: an old game account or your main email?

Answer: Your main email, because other services often send password-reset links to it.

Your notes: _____

Use unique passwords and passphrases

Password reuse turns one data breach into a problem across multiple accounts. A trustworthy password manager can help create and store a unique password for every site.

STEP-BY-STEP PRACTICE

1. Choose a reputable password manager and protect it using one long, memorable master passphrase that you have never used elsewhere.
2. For a test account, use the manager to generate a long random password. Never reuse a password from another website.
3. Change reused passwords for your most important accounts, starting with your primary email and domain registrar.
4. Check your account recovery settings and store recovery codes separately and securely.

KEY TAKEAWAY

Length, uniqueness, and safe recovery matter more than complicated character tricks.

CHECK YOUR KNOWLEDGE

Is one complicated password reused on six websites safer than six different passwords?

Answer: No. Six different strong passwords prevent a breach of one website from unlocking the others.

Your notes: _____

Turn on stronger sign-in protection

Multifactor authentication (MFA) adds an independent proof of identity. Passkeys and security keys are phishing-resistant options where available; authenticator apps are also widely useful.

STEP-BY-STEP PRACTICE

1. Open the security settings of one important account (for example Cloudflare or Namecheap).
2. Look for Passkeys, Two-Factor Authentication, or MFA. Choose a passkey/security key if practical, or an authenticator app.
3. Complete verification and sign out, then test signing in again before changing anything else.
4. Save recovery codes somewhere separate from the phone, and consider a second backup sign-in method. Never give anyone an MFA code.

KEY TAKEAWAY

An authenticator app works without cellular service, but account recovery still needs planning.

CHECK YOUR KNOWLEDGE

What should you do if a caller asks for your one-time login code?

Answer: Do not share it. Real support staff should not need your authentication code.

Your notes: _____

Keep devices updated and back up your data

Software updates fix security flaws. Backups reduce the impact of lost phones, mistakes, ransomware, and account problems.

STEP-BY-STEP PRACTICE

1. On your phone or computer, check Settings for operating-system updates and apply trusted updates when convenient.
2. Open your browser and major apps and confirm automatic updates are enabled.
3. Choose one small non-sensitive file and copy it to a separate location you control, such as a trusted cloud drive or external device.
4. Open the backup copy to verify it is readable. Write down how often you will repeat this check.

KEY TAKEAWAY

A backup is only useful after you confirm you can restore a file from it.

CHECK YOUR KNOWLEDGE

If files are syncing to one account, does that always count as a complete backup?

Answer: No. Syncing may also copy deletions or account changes. Keep a separate recoverable copy for important data.

Your notes: _____

PRACTICE CHECKLIST

- [] Lesson 1: Know what you need to protect
- [] Lesson 2: Use unique passwords and passphrases
- [] Lesson 3: Turn on stronger sign-in protection
- [] Lesson 4: Keep devices updated and back up your data

TRUSTED FURTHER READING

CISA: Secure Our World

<https://www.cisa.gov/secure-our-world>

NIST: Digital Identity Guidelines

<https://pages.nist.gov/800-63-4/sp800-63b.html>

Copyright © 2026 Black Cloud Security. Free for personal study and classroom sharing with credit. This material is educational and does not provide authorization to test any third-party systems.