

Security Awareness & Phishing

Real-world techniques to evaluate messages, verify links, and respond safely to suspicious activity.

WHAT YOU WILL LEARN

- Recognize phishing pressure tactics and spoofing
- Inspect domain names without opening suspicious links
- Respond to potential account compromise

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.

Spot common phishing warning signs

Phishing attempts persuade people to reveal information, send money, or open harmful links. Attackers often use urgency and impersonation.

STEP-BY-STEP PRACTICE

1. Imagine a message saying: "Your domain expires in 10 minutes! Sign in using this link."
2. Look for pressure, unusual sender details, unexpected requests for passwords, and strange domains.
3. Do not open the message link. Visit your domain registrar by typing the known address yourself.
4. If the renewal message is genuine, verify it within your trusted account dashboard.

KEY TAKEAWAY

Scammers can spoof names and logos, so visual appearance alone does not establish authenticity.

CHECK YOUR KNOWLEDGE

Should you trust an urgent renewal message because it displays a familiar logo?

Answer: No. Verify through the service website or app you already trust.

Your notes: _____

Read a URL carefully

Attackers may put a brand name in a subdomain or path to make a link look official. The registered domain is the crucial part of the address.

STEP-BY-STEP PRACTICE

1. Look at this harmless made-up example as text only: `https://cloudflare.example.net/security` (do not browse it as a Cloudflare page).
2. Identify that `example.net` is the registered domain; "cloudflare" is just a subdomain label.
3. Compare it with `https://dash.cloudflare.com`, where the registered domain is `cloudflare.com`.
4. Practice by examining, not visiting, three suspicious links. Never paste private reset or verification links into public scanners.

KEY TAKEAWAY

A brand name somewhere in a URL is not enough. Read the actual registered domain.

CHECK YOUR KNOWLEDGE

In `login.example.com.attacker.test`, is `example.com` the registered domain?

Answer: No. The final registered domain is `attacker.test` in this illustrative address.

Your notes: _____

Verify requests outside the message

Unexpected messages may claim to be from a bank, family member, delivery company, or technical support. Verification should not rely on contact information supplied in the same suspicious message.

STEP-BY-STEP PRACTICE

1. If a message requests money, codes, identity documents, or an urgent password reset, stop before responding.
2. Open the official app or type the known website address yourself; do not follow the message link.
3. Call a saved number or a number listed on a statement or official website.
4. Report the suspicious message using the service's built-in report button and remove it if appropriate.

KEY TAKEAWAY

Independent verification breaks the attacker's control over the conversation.

CHECK YOUR KNOWLEDGE

Which phone number should you use to verify a suspicious bank text?

Answer: A trusted number from the bank's official app, website, or bank statement—not the number in the text.

Your notes: _____

Respond if you clicked or shared information

Fast action can limit damage. The right response depends on whether you simply visited a page, installed something, or gave up a password or MFA code.

STEP-BY-STEP PRACTICE

1. Stop using the suspicious page. Do not download further files or enter additional information.
2. If you entered a password, open the real website directly and change it; also change that password anywhere else it was reused.
3. Review recent sign-ins, recovery methods, connected devices, and active sessions; sign out unknown sessions where supported.
4. If you installed software or suspect device compromise, disconnect when appropriate, update and scan the device with trusted tools, and contact official support. For financial loss, contact the bank promptly.

KEY TAKEAWAY

Keep a simple record of what happened, the time, affected accounts, and steps taken.

CHECK YOUR KNOWLEDGE

If you gave away an MFA recovery code, is changing only the password enough?

Answer: Not necessarily. Revoke/regenerate compromised recovery codes and review all sign-in methods and active sessions.

Your notes: _____

PRACTICE CHECKLIST

- [] Lesson 1: Spot common phishing warning signs
- [] Lesson 2: Read a URL carefully
- [] Lesson 3: Verify requests outside the message
- [] Lesson 4: Respond if you clicked or shared information

TRUSTED FURTHER READING

FTC: How to recognize phishing scams

<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

CISA: Recognize and report phishing

<https://www.cisa.gov/secure-our-world/recognize-and-report-phishing>

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.