INFORMATION TECHNOLOGY
COLORADO STATE UNIVERSITY SYSTEM

COLORADO STATE UNIVERSITY

Think Before You Click: A Student's Guide to Phishing

1

What is Phishing?

Phishing is when someone **pretends** to be a trusted person or site to get you to reveal information or run a file. It works because it plays on **feelings, urgency, curiosity,** FOMO, not on fancy hacking. Attackers can buy ready-made phishing kits and services, so you're being targeted by a whole business model, not just a bored prankster.

2

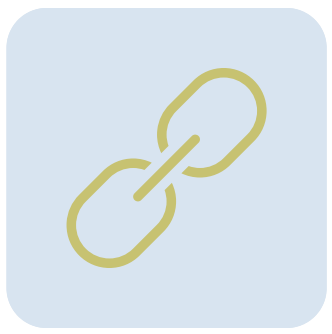
Quick Campus Examples

• An email that looks like it's from Canvas, a campus IT alert, or a professor asking you to "confirm your password."
• A mysterious QR code on a flyer promising free pizza or event tickets (this is called quishing).
• A text message or voicemail asking for your two-factor code (smishing / vishing).

3

How Phishing Tricks You

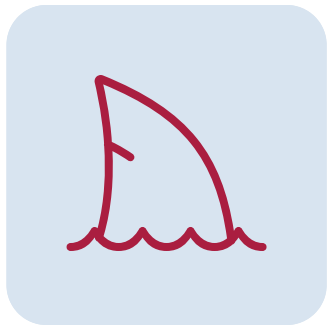
1. Text or link masking, Link text says "official site," but the real URL sends you somewhere else. Hover your mouse (or long-press on mobile) to preview the real link. 2. URL/subdomain tricks, Attackers register look-similar domains (e.g., microscft-login.com) or use subdomains like login.amazon.com.badsite.net to make things look legit. Always check the real domain.



4

Types to Watch For

• Spear / whaling: highly targeted emails (professors, student org leaders).
• Smishing / vishing: texts or phone calls asking for info.
• Quishing: malicious QR codes.
• Clone / fake login pages: looks like the real login but steals your credentials.



5

Quick Safety Checklist

• Hover or long-press links to see the real URL before you click. • Don't scan random QR codes, type the official site or use the app instead. • Use multi-factor authentication (MFA) on school and personal accounts. • Verify urgent requests: call the sender or message them through a known channel. • Use strong, unique passwords (password manager recommended). • Keep your device and browser up to date and run antivirus scans when needed.

6

If You Clicked or Gave Info

1. Disconnect from Wi-Fi (stop ongoing data leak).
2. Change the password for that account from a different device and revoke any active sessions.
3. Turn on/confirm MFA on the affected account.
4. Report it: forward the phishing email to your email provider and notify campus IT/security.
5. Run a malware scan and watch your accounts and bank statements for suspicious activity.

7

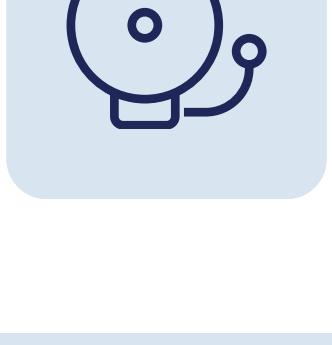
Common Campus Tricks

• Fake Campus/IT Emails: Urgent course alerts or password confirmation requests
• QR Codes on Flyers: Promising free food, tickets, or other campus perks
• Smishing & Vishing: Texts or voicemails asking for verification codes
• Clone Login Pages: Perfect copies of campus login portals designed to steal credentials

8

Why It Matters

Even "small" credentials are sold and reused. Attackers often sell initial access or use your account to phish others. One compromised student account can help attackers move laterally inside campus systems. that's how big breaches start. Final quick tip: When in doubt, slow down. Attackers rely on rushed decisions and curiosity. A five-second check can save you hours of cleanup.



Short version: Phishing is social engineering that tricks you into clicking links, handing over passwords, or downloading malware. It's easy for attackers, and one click can cost you a lot.