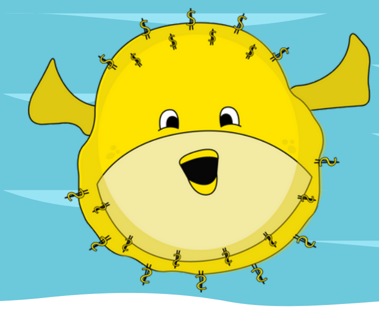

PAYMENT PERRY

Protect your payment info from Phil!

Don’t Click

Always double-check the sender's email or message. Phishing scams often come disguised as banks or trusted companies. If you're unsure, go directly to the website by typing the URL yourself instead of clicking links.

Use MFA

Enable MFA (multi-factor authentication) on your financial accounts whenever possible. This adds an extra layer of security, making it harder for attackers to access your account even if they get your login credentials.

Update Software

Regularly update your browser, antivirus software, and operating system. Security patches help protect you from the latest phishing tactics and malware designed to steal your payment data.

Monitor

Monitor bank and credit statements and regularly check your accounts for unauthorized charges. Early detection allows you to report and stop fraudulent activity quickly.

Don’t Share

Never share payment info over email or text. Legitimate companies will never ask you to send credit card or banking details through email, text, or messaging apps. If you receive such a request, it’s likely a scam.

RESOURCES

- cisa.gov/shields-up
- usa.gov/scams-and-fraud
- cisa.gov/secure-our-world

cyberhouserock.info