

Clickbait and Phishing

Clickbait and phishing (said like fishing) are two big scams—let's practice how to spot them.

1. Use the words below to fill in the missing vocabulary on internet safety.

phishing
email

sensitive
credit card

corrupt files
account

information
passwords

clickbait
malware

Phishing occurs when scammers send emails or texts that try to trick the user into revealing sensitive information. These scammers will use a tone of urgency to get you to enter your account information, credit card information, and passwords. Common techniques they'll use include clickbait, attaching, corrupt files and asking you to verify your email address.

2. Scammers use clickbait to attract your attention and get you to click on a corrupt link. Which of these could be an example of clickbait? (Circle all that apply)

- a. Please verify you are not a robot by entering the following characters.
- b. Click [Claim Now] to claim your prize.
- c. Call us with any questions
- ☒ d. Urgent Notice! "Click Here to prevent further damage to your device."

3. Circle any phishy parts in the contents of this e-mail.

Portnight IT <dubedu@business-real.uk>
Monday, August 13, 2024 at 10:00 PM

URGENT MESSAGE!

Your Portnight account has been compromised. Several purchases have been made from an unknown device. Open the attached file to view these purchases.

Didn't make these purchases?
Click here to verify your account details and report stolen information.

↓ **Fkeport_Invoice.pdf**
— 2014 KB

4. What do you think you should do if you're the victim of clickbait or phishing?

Change your passwords, contact the organization that was spoofed, scan your computer for viruses, file a report with the FTC (Federal Trade Commission), and/or protect yourself in the future.