Oops!

Powered by PHIN

You clicked a scam... now what?

1) Breathe

2) Notify IT immediately

Not every click is a code red

(But you should still *always* report it to IT immediately).

Just clicked

Many phishing websites are designed to steal credentials rather than infect devices automatically.

Entered your password

Assume your credentials have been compromised and change your password for that account immediately. You should also ensure that MFA is enabled. *Note: You should never reuse the same password on multiple sites. Once that password is confiscated, all of your accounts with the same password are in jeopardy.

Downloaded a file

Contact IT immediately and follow their guidance, which usually includes disconnecting from the internet. Not all downloads are malicious, but you should always assume it's guilty until proven innocent (unlike jury duty).

Keep an eye out for warning signs

- Unexpected pop-ups
- Programs opening on their own
- Significant slowdowns
- Browser redirects
- Unusual login prompts
- Applications crashing unexpectedly
- Password reset emails you didn't request
- Messages sent from your account that you didn't write
- Unexpected MFA prompts
- Financial transactions or account changes you don't recognize