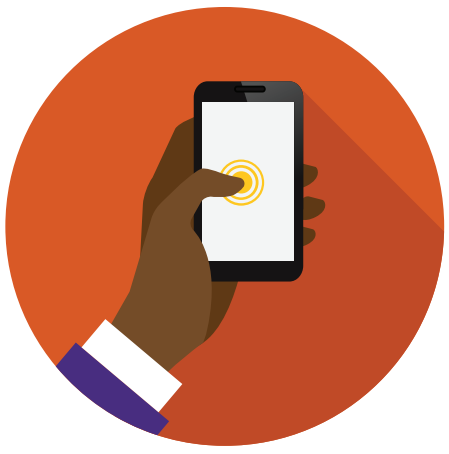
HOOK, LINE & SINKER

The tricks hackers use to try to get your personal information and how to avoid it.

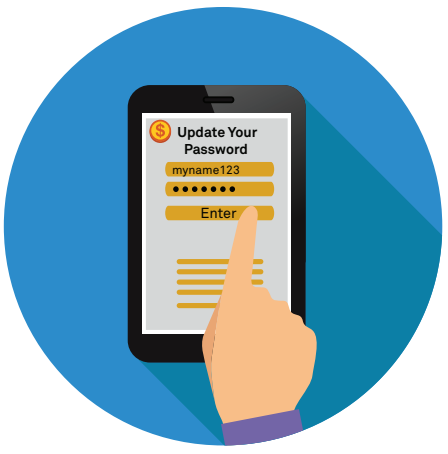
Common Phishing Tactics

Phishing happens when you get an email from what looks like a trusted source (such as Northwestern or your bank) asking for personal information.

Messages are often urgent or threatening



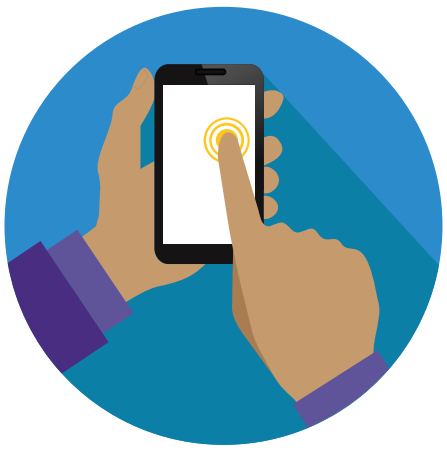
You may be asked to click a link or open an attachment to verify information



Graphics, URLs, and signatures often look legitimate

What to Do if You Suspect Phishing

The "phishing" lure may look convincing, but don't take the bait



Don't open attachments or click email links unless you know they are legitimate

Check for odd sender email addresses or misspellings

Search for the real website online and confirm its address

Do not reply or send passwords or other personal information

Not sure? Forward a copy of the email to security@northwestern.edu

Delete messages you confirm to be phishing attempts from your inbox

Uh-Oh, did you get hooked?

If you think you may have clicked something suspicious, let us know—we're here to help: **security@northwestern.edu**