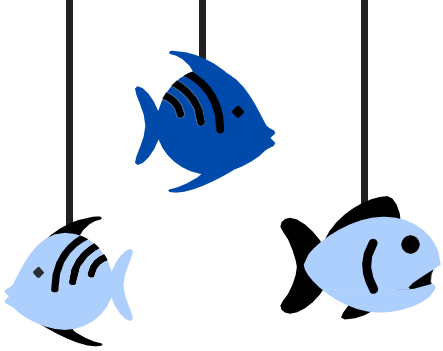
Helpful Tips to Avoid the *PHISH*



While information security controls prevent a large amount of phishing attacks, they can't catch them all, and some scam emails still make it into our inboxes. Our best defense against phishing attacks is YOU! Review the tips below to avoid falling victim to cybercriminals attempts.

- **Verify the sender** (domain, tone, contact recognition).
- If it is **not work-related**, delete it!
- Be suspicious of **urgent demand**s or other frightening language.
- Watch for **grammatical/spelling errors** or **generic wording** or responses that do not answer your questions.
- Hover over links to **verify address** authenticity.
- **Review attachment file names**. If you weren't expecting them, be cautious.
- Listen to yourself. If something just **doesn't "feel right",** verify it first.
- If it seems **too good to be true**, it probably is.
- **Ask a coworker** for help!
- **Do not mark suspicious emails as junk or spam**. Just delete them.
- **Don't set up rules** to move suspicious emails into certain folders.
- **Do not forward the email** to anyone outside of IT.
- **If available, report suspicious emails using the Phish Alert button**.
- If you have email on your phone:
  - Wait until you have **access to a computer** for easier viewing of suspicious emails.
  - Use the **Outlook or Gmail app** on your mobile device, not the general email application.
  - Keep your **work and personal emails separate**.
  - Be careful of other application permissions you are giving. Some applications request your permissions to access your emails, which can automatically open any attachments you receive.

If any suspicious indicators are present in an email, pause and think before taking action. If something does not seem right, report it to help keep our organization safe from phishing