Fight the Phish

Phishing and social engineering are the most common form of cyber attacks. According to FTI Consulting's 2021 Resilience Barometer® survey, more than **1 in 3 respondents** were negatively affected by phishing attacks in the last 12 months – up from 29% in 2020.

What is Phishing?

The attempt to illegally solicit information through email, text messages, or other forms of communication.

This can be achieved through the deceptive transmission of informational requests, as well as the fraudulent misrepresentation of the perpetrator as an official, privileged party for such information.

Criminals use phishing to obtain:

- Passwords & account information
- Money
- Network access

How to Spot the Phish

The email address is not a company email, or it contains a deceptive misspelling to appear like an authentic email.

The message was sent unexpectedly.

The message contains:

- Threatening or urgent language; spelling and/or grammatical errors
- A suspicious link or attachment
- A request for sensitive information, such as passwords, Social Security numbers, or payment information

Don't Take the Bait

- Check the legitimacy of the sender
- Verify the link location by hovering over the hyperlink
- Do not open or download attachments until you have verified the sender
- Call the sender to validate the email request if it is suspicious
- Report any suspicious emails to your IT department