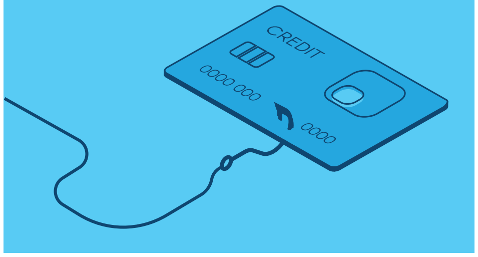
CYBERSECURITY / #01

PHISHING

A type of fraud in which emails pretending to be from reputable companies attempt to trick victims into providing personal data, such as passwords and credit card numbers.

NEVER GIVE PERSONAL INFORMATION

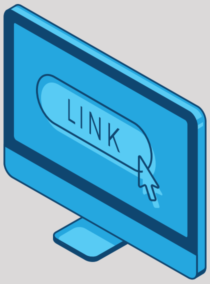
Most legitimate companies will never ask for personal credentials via email. Asking to change or verify sensitive information is a tactic used to scare the end user into clicking on a bad link or going to a bad site and filling in account information.



BE WARY OF .EXE ATTACHMENTS

HOVER OVER LINKS

Verify where links will actually take you to by hovering over the link. Do not click links, open attachments, or fill out forms in suspicious emails.



CHECK THE SOURCE

Hover over the "from" display name to inspect the sender's email address. Attackers commonly switch, add, or replace characters in their email address to appear legitimate.

BE CAUTIOUS OF URGENCY

Hackers word emails to include a sense of urgency to make you react quickly, reducing your time to think and realize the scam.

WATCH FOR UNUSUAL "PHRASES OR GRAMMAR"

DON'T BE FOOLED BY LOGOS

Logos and brand names of established companies are used to create a sense of trust. Check if the email signature looks legitimate and provides contact information.

TYPES OF PHISH BAIT

- EMAIL PHISHING
- PHONE CALL (Vishing)
- TEXT MESSAGE (SMiShing)
- USB BAITING

EAST BATON ROUGE PARISH LIBRARY

RED STICK READY

CITY OF BATON ROUGE
PARISH OF EAST BATON ROUGE
BR