WHAT IS PHISHING?

Fidelity Bank
Right By You.

Phishing is when criminals send convincing looking, but fraudulent emails, or make phone calls, to lure you into providing your confidential information, such as debit card numbers, social security numbers, or other non-public information for the purpose of defrauding an online account holder. Fraudsters use the information you provide to access your accounts and money or to steal your identity. Criminals can also use hyperlinks or attached files within phishing emails as a way to infect your computer or device with malicious software (malware).

Here's how to spot a phishing scam:

When you receive an email, check it for signs that it may not be from the company it appears to be from.

- **Check the email address** - Is it the same as the email address you usually receive emails from, or just similar?
- **Look for an emotive prompt** to click on a hyperlink or a button or to download a file, such as 'Verify your account or password' or 'update your security details'. This will likely take you to a copycat website where you will be prompted to enter your full details.
- **Be suspicious of any message that creates a sense of urgency**, such as 'If you don't respond within 48 hours, your account will be suspended'. A legitimate company will not create a false sense of urgency.
- **Check the wording** for casual or informal words.
- **Check the grammar and spelling** for mistakes or inconsistencies.

Phishing can also take place during phone calls. Below are a few tips to help prevent you from becoming a victim of fraud.

- Never give your full PIN or Online/Telephone Banking login details to anyone, even a caller claiming to be from your bank or the police. If you get a call asking you for this information, end the call immediately.
- If you receive a suspicious or unexpected call, always verify the caller, the purpose of the call, and the phone number the person is calling from.