Email Safety & Phishing Awareness

A practical security guide for individuals, businesses, and ministries.

Prepared by **LaFaries Mortimer LLC** — Administrative & IT Services

This guide teaches you how to recognize malicious emails, avoid common phishing traps, and protect your personal and organizational information with confidence.

1. What Is Phishing?

Phishing is a form of cyber attack where criminals impersonate legitimate organizations or individuals to trick you into revealing sensitive information such as passwords, financial details, or login credentials.

These attacks most commonly arrive by email, but may also appear via text message, social media, or phone calls.

2. Common Phishing Red Flags

Watch for urgent language, unexpected attachments, spelling or grammar mistakes, generic greetings, suspicious sender addresses, and links that do not match the displayed text.

3. Email Types That Require Extra Caution

Be especially cautious with emails related to password resets, invoices, delivery notices, bank alerts, tax notifications, or messages claiming your account will be closed.

4. How to Safely Handle Suspicious Emails

Do not click links or download attachments from suspicious emails. Verify the message by contacting the organization directly using a trusted method.

If unsure, forward the message to your IT administrator or delete it immediately.

5. Best Practices for Email Security

Use strong, unique passwords, enable multi-factor authentication, keep your devices updated, and never reuse work credentials for personal accounts.

6. What To Do If You Clicked a Phishing Link

Immediately disconnect from the internet, change your passwords, and notify your IT provider or administrator. Early action can prevent further damage.

Security awareness is not about fear — it is about preparation. Staying informed protects you, your organization, and the people you serve.