Phish & Clicks

You need some help with: Recognizing Phishing Emails

Phishing emails are often designed to trick you into clicking malicious links or sharing sensitive information. Below is an example of how phishing emails typically operate, with key tactics highlighted to help you identify them:

Example Phishing Email:

Dear User,

Urgent: Your account has been compromised!

⟶ **Click here** to verify your identity and recover your account.

⟶ **This is a time-sensitive matter!**

Sincerely,
Your Bank

Key Tactics Used in Phishing Emails:

- ⟶ **Urgency or Fear:** The email creates a sense of urgency (e.g., "Your account has been compromised" or "Immediate action required") to push you to act quickly without thinking.
- ⟶ **Suspicious Links:** The "Click here" link often redirects you to a fake website designed to steal your personal information.
- ⟶ **Generic Greetings:** Phishing emails often use generic phrases like "Dear User" or "Dear Customer" instead of using your name.
- ⟶ **Unusual Sender:** The sender's email address may look suspicious or unfamiliar, with small changes to a trusted domain name (e.g., banktrust-xyz.com instead of banktrust.com).

Important Tip:

Always verify the sender's email address, hover over links to check their destination, and contact the company directly through official channels if you are unsure of an email's authenticity.

How to Protect Yourself:

- Always double-check the source of emails before clicking on any link.
- Never provide sensitive information like passwords or credit card details via email.
- Report suspicious emails to your IT department or email provider immediately.

If you need help identifying phishing emails or if you suspect an email is phishing, please contact support at support@phish-n-clicks.com.