Phishing emails

Phishing refers to the process of deceiving recipients into sharing sensitive information with an unknown third party (cyber criminal).

Typically in a phishing email scam, you receive an email that appears to come from a reputable organization, such as:

- Banks
- Social media (Facebook, Twitter)
- Online games
- Online services with access to your financial information (e.g., iTunes, student loans, accounting services)
- Departments in your own organization (from your technical support team, system administrator, help desk, etc.)

To protect against phishing attacks, it's good practice not to click on links in email messages. Instead, you should enter the website address in the address field and then navigate to the correct page, or use a bookmark or a Favorite link. Phishing emails may also include attachments, which if opened can infect the machine.

Anti-phishing software can block many phishing-related emails.