Information Security Basics

Rev. 2025

Email & Phishing Safety

- Only open email attachments or click links if you are expecting them and know they are legitimate.
- Instead of clicking embedded links, **type the website address manually** into your browser.
- Never click "Unsubscribe" in suspicious emails; instead, **mark as Junk and Block Sender**.
- Emails with **.zip or .exe attachments** are extremely dangerous—verify with IT before opening.
- Be alert for **Phishing emails** that:
    - Ask you to confirm personal information
    - Demand immediate action or threaten account closure
- **Do not send sensitive information** via unencrypted email.
- To verify a suspicious email, **contact the organization directly**—never use the number or link in the email.
- Report phishing emails to IT or the designated security contact.

Passwords & Device Security

- Use a **different password** for each device, website, or software.
- Passwords should be at least 8 characters and include **numbers, lowercase, uppercase, and special characters**.
- **Never auto-save passwords** on devices or browsers.
- Enable **multi-factor authentication (MFA)** wherever possible.
- Keep devices updated with the latest **anti-virus, anti-spyware, and anti-adware software**.
- **Keep all operating systems and applications up-to-date.**

Internet & Wi-Fi Safety

- Avoid public Wi-Fi for sensitive transactions (banking, credit cards, etc.).
    - If necessary, use a secure VPN.
- Do not respond to **pop-ups or ads** promising cash, gift cards, or surveys.
- Look for **"https"** when entering sensitive information online—the "s" indicates the connection is secure.

Social Media & Email Use

- Use discretion when posting personal information online; attackers use this for **spear phishing**.
- Never use your **work email** for personal websites or accounts.

Physical & Document Security

- **Shred** sensitive documents (statements, expired cards, medical/insurance forms) before disposal.
- Avoid using **public charging stations**; connect devices only with your own AC adapter.

Phone & Scam Awareness

- Be cautious with unsolicited calls demanding payment.
- The **IRS or legitimate companies will never demand immediate payment by phone**.
- Hang up and call the company using verified contact information.

Additional Tips

- Back up important files regularly.
- Report any suspicious activity immediately to IT or the designated security contact.