Cybersecurity Updates

Ransomware Overview

- **Definition**: Typically encrypts all data on a disk and can expand to network data.

- **Decryption Difficulty**:

  - Virtually impossible to decrypt; a supercomputer would need $105110^{51}1051$ years to decrypt a single word.

Immediate Actions If Infected

- **Disconnect Immediately**:

  - Unplug Ethernet cable.

  - Turn off Wi-Fi (via Windows icon or physical switch).

  - Unplug external drives like flash and hard drives.

- **Document the Issue**:

  - Take a photo of the ransom note.

Removing the Ransomware

- **Important Note**: Must remove ransomware software before attempting any recovery.

- **Procedure**:

  - Reboot into safe mode and run antivirus software.

  - Seek professional help.

Recovery Options

- **Recover From Backups**:

  - Preferred method using on-premise or cloud backups.

  - **Risks**: If ransomware is active, it might encrypt the backups.

  - **Types of Backups**:

    - On-premises.

    - Cloud backups with air gaps.

- **Attempt Decryption**:

  - Identify the ransomware strain; some have known keys.

  - **Website for Help**: No More Ransom.

- o **Risks**: Incorrect decryption can permanently damage files.

- **Pay the Ransom**:

  - o Typically demanded in cryptocurrency.

  - o **Advised Against**: High risk of loss without guaranteed decryption.

- **Give Up, Start Over**:

  - o Humorous take on losing data and starting afresh with better habits.

Prevention Tips

- **Regular Updates**:

  - o Promptly apply software and Windows updates.

- **Antivirus and Adblocker**:

  - o Windows Defender and options like Eset or Bitdefender.

  - o Recommended adblocker: uBlock Origin.

- **Be Wary of Scams**:

  - o Typical email scams involve altered banking information.

  - o **Preventive Steps**:

    - Verify changes via phone.

    - Dual approval for wire transfers.

    - Delay transactions to allow time for verification.

Cyber Insurance

- **Coverage Explained**:

  - o Differentiates between first-party and third-party liabilities.

- **Options**:

  - o Cyber Security Companies: Offer prevention help but are costly.

  - o Traditional Insurance: High coverage limits but complex and expensive.

- **Insurance Details**:

  - o Differences between retention and deductible.

  - o Coverage includes breach response, cyber extortion, and more.

Password Management

- **Current State**:

- Weak passwords are common and pose significant security risks.
- **Suggestions for Strong Passwords**:
    - Use lengthy, nonsensical phrases or sentences.
    - Include numbers, symbols, and capital letters.