RC CyberEdge

Day 3: Phishing, Online Scams, Malware and Viruses

A Cyber Heroes Activity

Day 3: Identifying Cyber Threats

Lesson:

- **Understanding phishing, scams, and malware.**
  - **Phishing:** Tricking people into giving up personal information (passwords, credit card details) by pretending to be a trustworthy entity. **– Scams:** Deceptive schemes designed to defraud people.
  - **Malware:** Malicious software designed to damage or disrupt computer systems. This includes viruses, spyware, and ransomware.
- **How to spot suspicious messages and avoid them.**

Activity: Cyber Detective Mission - Sample Messages Instructions:
Analyze each of the following messages and determine if they are safe or suspicious. Provide a brief explanation for your decision, highlighting any red flags or indicators of potential cyber threats. **Messages:**

1. **Text Message:**
   - ”Congrats! You’ve won a free iPhone! Click here to claim your prize:

     bit.ly/2AbCdEfGhIjKlMnOpQrStUvWxYz”
2. **Social Media Post:**
   - ”Reminder: School picture day is this Wednesday! Wear your best smile! #SchoolPhotos #PictureDay” - Jane Doe
3. **Website Pop-Up:**
   - ”Your computer has a virus! Download our free antivirus software now! free-antivirus-download.malware.com/install” - Robert Martinez

Answer Key and Discussion Points (for Teachers):

1. **Text Message (Suspicious):**
   - **Explanation:** This message is highly suspicious due to the ”too good-to-be-true” offer of a free iPhone. The shortened link (bit.ly) is a common tactic used by scammers to hide the actual destination URL, which could lead to a phishing site or malware download.
   - **Red Flags:** Unsolicited message, unrealistic offer, shortened link.
2. **Social Media Post (Safe):**
   - **Explanation:** This message is safe because it comes from a known source (Jane Doe, presumably a school administrator), provides clear and relevant information about a school event, and uses relevant hashtags.
   - **Indicators of Safety:** Known sender, clear context, relevant hashtags.

3. **Website Pop-Up (Suspicious):**

- **Explanation:** This message is suspicious due to the urgent and alarming claim of a computer virus, coupled with an unsolicited offer to download "free antivirus software." The domain malware.com is a significant red flag.
- **Red Flags:** Urgent warning, unsolicited offer, suspicious domain name.

How to Use in the Activity:

- **Print or Display:** Print these messages or display them on a screen for students to analyze.
- **Analysis:** Have students individually or in groups analyze each message and write down whether they think it's safe or suspicious, along with their reasoning.
- **Discussion:** After the analysis, facilitate a class discussion to review the messages and discuss the students' findings.
- **Reinforcement:** Emphasize the importance of being cautious and critical when encountering messages, especially those with suspicious links or alarming claims.

By using these examples, you provide a clear and practical way for students to learn how to identify cyber threats.