Phishing: Don't Be Phooled!

Top Tips for Healthcare Organizations

1. **Raise the collective PHISHING IQ of everyone ✓**
   a. Provide security awareness and phishing education and training
   b. Consider adopting awareness initiatives: Data Privacy Day, National Cyber Security Awareness Month, and Stay Safe Online
2. **Train workers to be SUPICIOUS 🔎**
   a. Look for mistakes in the message (e.g., spelling, grammar, factual, etc.)
   b. Watch out for 0dd l00king characters, including in the message, links, and elsewhere
3. **Train workers to be CAUTIOUS ⚠**
   a. Look out for messages that ask for personal, confidential, sensitive, proprietary, or employee information
4. **Train workers to TRUST their INSTINCTS & COMMON SENSE !**
   a. If the message seems suspicious or odd, err on the side of caution
   b. Question special requests from C-suite executives (e.g., CFO, CEO), coworkers, vendors, others
5. **Verify emails with the SENDER ✉**
   a. Contact the sender via an out-of-band communication channel (e.g., telephone call or otherwise) to verify the contents of a message
6. **Never CLICK links if you are unsure about where they lead 💣**
   a. Expand shortened links to determine if it is malicious
   b. Check to see if the text of the link matches the actual embedded link
7. **Always REPORT phishing emails ☎**
   a. Forward the message as an attachment to your organization's point of contact
   b. Inform co-workers and engage with others about phishing
8. **IMPLEMENT basic & advanced security controls 💯**
   a. Practice defense in depth with human & technical controls

2018 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Vulnerabilities of Healthcare Information Technology Systems