SAFE COMPUTING/E-MAIL/WEBSITE TIPS @ POBCSD

Clicking While Computing: What You Should Always Be Aware Of

Guy A. Lodico, Director of Technology

As our District is constantly in the process of proactively stopping and neutralizing malicious virus/Trojan/worm type threats that attempt to propagate our network on an ongoing basis, I would like to remind all POBCSD network users of the following best practices that will continue to help safeguard both your home and district networked computers against malicious network threats such as E-mail scams, viruses/Trojans/worms/spyware, and spam, for example.

1. **Screen messages before viewing them, and delete anything that appears suspicious:**
   - **Carefully examine your list of unopened E-mail messages.**
     Do any of your unopened e-mail messages come from people or addresses you don't recognize? Do the subject lines have words with too many spaces, or long random numbers? Do they seem too good to be true, or somehow odd? If so, it's probably best to just delete the message along with any attachments and contact the sender in another way to verify the content of the message prior to opening.
   - **Wait! Don't open that email yet...**
     If a message has attachments don't open them unless you know the sender and/or are expecting the attachment. If you're not sure what it is, as an extra precaution, again, contact the sender before opening the message and ask exactly what the message and attachment is all about
   - **Don't be fooled by E-mail tricks.**
     Most computer worms (a kind of malicious program) spread themselves via email by spoofing addresses found in the infected computer's address book and sending copies of itself to other addresses in the address book, so it's very likely that an infected message can appear to come from someone you know. Many of these messages will use vague or generic subject lines like "Re:" or "Hi." Others will try to look like they came from a technical support service, or even from Microsoft or Apple. Be extra careful about opening these. *IMPORTANT NOTE:* ***The only network alert E-mails you will receive regarding our POBCSD network will come from either myself (Guy Lodico) or Michele Zeplin as the identified sender. Our District's Central Office of Technology will never identify a potential network issue with the sender's name being generically addressed as "administrator" – "network administrator" - "techsupport" - "Microsoft" - etc*****.**

2. **Open your messages, but beware the next and previous buttons.**
   - Using the Next and Previous buttons to open and move from message to message is convenient but could potentially be dangerous, especially if you don't screen messages thoroughly, or if new messages come in while you're reading other screened messages.

3. **Handle attachments and advertised Web-links with care: Chances are what appears to be a joke is NO JOKE!**
   - **Don't open attachments unless you are absolutely sure about what they are and who they came from.** Even attachments that were sent directly to you by a known sender might contain malicious code. **Many threats come in as Trojans, for example, disguised as an inviting link to what appears to be an innocent JOKE. Chances are it's no joke!!!!!!!!!**
   - **Be aware of Dangerous File Types!**
     Some file types have been deemed unsafe by Microsoft. Most of these file types are executable or exploitable and are considered unsafe to send and receive as email attachments. Our POBCSD network continually scans all incoming e-mail messages for attachments using any unsafe file types and takes every measure to block them before they can cause harm to our computers and network.
   - Some malicious attachments will "pose" as a harmless file type like a digital image/video by including that file type extension in it's name. You might get an attachment called "Important.jpg" and think it's a picture from someone you think you know. But it might actually be one of the exploitable file types. Once again, many threats come in as Trojans disguised as links to what appears to be an innocent JOKE***. NOT ONLY WILL THESE JOKE-TYPE LINKS POTENTIALLY THREATEN OUR NETWORKS THEY SHOULD NOT BE SPREAD USING DISTRICT RESOURCES AT ALL IN ALIGMENT WITH USER SIGNED DISTRICT POLICIES.***

4. **Be aware of E-mail and Website Hyperlinks:**
   - Another popular scam always propagating the Internet is E-mail and Website scams that try to bait you into clicking on an embedded hyperlink. For example, it might read ***"click here to update your personal bank account information"*** **or "*If the message is not displayed automatically, follow the link to read the delivered message. Received message is available at: pobschools-org/inbox/yourname/read.php?sessionid-32497.*"** Notice in this example that the scammer has used our familiar "www.pobschools.org + your own name" as the spoofed address is trying to trick you into thinking it is a legitimate link. Don't click on it – it's potentially another scam and inevitably another potential threat and problem for our networks.