

Information Technology: 10 Steps Users Should Follow to Help Protect Your Financial Institution

Jay Butler, Senior Technical Consultant, Safe Systems, Inc.

- 1. Keep on the lookout for any suspicious activity.** For example, a recent email attack attempted to coax end users into opening an attachment by informing the recipient that her mailbox settings needed updating. A common sign of suspicious email is format and grammar. The subject of the email message read this way: “Subject: **Setting** for your mailbox **are** changed.” Notice “**Setting**” and “**are**” are grammatically incompatible here. The common verbiage would say “Subject: Settings for your mailbox have changed.” Unusually incorrect grammar and misspellings are very common in dubious email. Another oddity in this example was the attachment itself. It was an Adobe .pdf file that the email claimed was instructions, but instead it launched a program when the user opened it. The program ran the actual attack against the computer if the user answered the prompt to continue after opening the .pdf attachment. Immediately report any suspicious activity to the appropriate personnel such as your manager, security officer, Systems Administrator, or Safe Systems, Inc. If you make a mistake, do not be embarrassed and decide to keep it quiet. The scammers are experts in the art of deception, so anyone can fall prey to their tricks. Report it immediately to minimize damage and help others do the same.
- 2. Never click on any pop-up message that asks to scan your machine.** For example, a notorious piece of malware appeared as a legitimate antivirus scan but it was actually a rogue program designed to lure users into buying the full version (example shown below). It would also negatively affect the performance of infected computers. Note that your actual corporate antivirus solution typically does not prompt you to perform any action. It occurs “behind the scenes” unless your administrator has notified you otherwise. Thus, if you are ever prompted to run a virus scan, cancel the operation and contact your Systems Administrator.



Figure 1: Fake antivirus scan.

3. **Only open legitimate email. Permanently delete spam.** Carefully highlight and permanently delete using <shift> delete like this: After highlighting the message(s), right click the selection(s) so the menu appears. Hold down the <shift> key before clicking the delete option from the menu. Choose Yes to permanently delete the messages.
4. **Do NOT click links found in email messages or other documents even in legitimate looking email.** Instead, carefully copy the text and paste it into the address field of Internet Explorer, or better yet just type it out. A link appearing to be a perfectly legitimate web address can actually take you to a fake website that mimics the real one. A fake website designed to mimic the actual website in order to steal information is a form of Phishing.
5. **Never (ever) give out usernames or passwords in an email or over the phone.** A hacker can easily impersonate email or voice from someone you trust such as your Systems Administrator or even a CEO. Guard other private information using the same logic.
6. **Avoid transmitting any private information electronically through medium such as email, phone, instant messengers (chat), text messages, or social networks (Facebook).** If your institution has encrypted email, be sure you understand how to use it. Encrypted email is an exception to this rule as long as it is encrypted using the right system.
7. **Do not click on any pop-up window that asks you to download, run, install or update unless you have been notified otherwise by your administrator.** This practice dramatically reduces the chance of any rogue software infiltrating your computer.
8. **Avoid non-business related websites when using corporate owned equipment.** Understand that most financial institutions monitor all websites you access. Avoid any embarrassment or worse by keeping it business related. Risk of infection increases exponentially when surfing any non-business related website or when using any non-business related software.
9. **If you're allowed to use chat software at work such as Yahoo Instant Messaging or Microsoft Live Messenger, be cautious. Do not click on any links within chat sessions or type any private information even when speaking with a trusted source.** Much like email, a link may appear to be unsuspecting but may actually be a cyber attack. Type it out manually instead. Never download or install anything over a chat session. Use chat software only for its original intent, chatting. If it is something private, use an alternate medium such as the phone or an encrypted email. Hackers can impersonate chat contacts as well.
10. **Do not download or install any software on your machine without management approval.**