10 Most Dangerous Things Users Do Online

So who is the single greatest threat to network security? Your Users of course.

Because, in the end, most users have no idea how dangerous their online behavior is. No matter how many times you train them, no matter how many classes you hold, most Technology professionals still watch helplessly as end users introduce new malware because they "just couldn't resist looking at the attachment." Security pros cringe as their users download software for personal use, turn off firewalls to speed up a connection, or leave their passwords stuck to their laptops.

What if we had a list of the top 10 things you should not do on line? Well here you go.

1. Clicking on email attachments from unknown senders

We know, we know. Haven't we beaten this one to death already? With all the computer training courses, news reports, magazine articles, and memos from the Tech department, are there any users left out there who don't know they aren't supposed to open email attachments from strangers? Even with today's new range of exploits, email attachments are still the most likely means of contracting viruses, worms, Trojan horses, and other infections. The problem isn't that users don't know the risks — it's that they can't help themselves.

2. Installing unauthorized applications

What do you mean, "no IM?"

If you're like many school districts today, prohibiting instant messaging is out of the question. IM is rapidly becoming a standard educational communication tool, even as the number of IM exploits rises. Like any other peer-to-peer application, instant messaging comes with some serious risks, but once your users are hooked on IM, they are hooked.

The "Best Practice" is to lock it down so that IM stays within the confines of the network. In other words, don't allow IM to others on the Internet, only within the school district.

3. Turning off or disabling automated security tools

Every day, users reschedule automated virus updates, remote security patch installations, or requests to change their passwords. Security stuff, they say, is an administrative hassle and keeps them from doing their "important" work.

Users that "work around" the security put the entire school district at risk.

4. Opening HTML or plain-text messages from unknown senders

While most end users today are aware, if not respectful, of the dangers associated with opening email attachments from strangers, many are not aware of the threats that may lie in a normal, everyday text or HTML message that contains no enclosure. Most of these users are those who have not updated their computer knowledge lately, and still labor under the illusion that only email attachments can contain malware.

HTML files may contain Java Scripts, ActiveX controls, or macros that can allow an attacker to gain control of a PC or turn it into a botnet zombie. The vast majority of Web pages contain one or more types of active content, with an unmistakable trend toward increasing use of active content in Web pages.

5. Surfing gambling, porn, or other legally-risky sites

One of the oldest abuses of Internet links, the downloading of porn, gambling and other objectionable data is another still-popular activity that falls into the "I thought we had that fixed" category.

6. Giving out passwords to other users

The password problem is as old as computers themselves. Despite years of trying, however, no one has come up with a workable solution. Staff members still write down passwords on sticky notes and locate them close to their workstation. Worse, passwords are not strong. Using strong passwords that have at least 8 characters with a combination of upper and lower case plus special characters is the best practice. *Using your school's mascot name for a password is out of the question.*

7. Random surfing of unknown, untrusted Websites

Browser-based vulnerabilities are becoming one of the most popular targets of attackers on the Web. Just ask Microsoft which has been busy patching new vulnerabilities each month. If you give users free reign to surf the Web during or after business hours from the school network, beware.

In addition to the well-documented cross-site scripting (XSS) vulnerabilities floating around, there's also a lot of adware and spyware. You shouldn't put it past that trusted student or employee to download some free music, for instance, and inadvertently contract some malware as a result.

8. Attaching to an unknown, untrustworthy WiFi network

There's nothing more soothing than a good cup of java and a free WiFi connection at your local coffee shop. But watch that guy at the booth next door — he may be hacking into your laptop over that very same WiFi link.

9. Filling out Web scripts, forms, or registration pages

If your users could actually see a hacker looking over their shoulder as they logged onto a Website or typed sensitive data into a registration page, maybe then they would think twice. But since keyloggers and XSS don't have a human face, you'd better hope your users are hanging out on SSL-secured sites — and know just what constitutes sensitive school district data.

Users are more likely to get hacked if they use the same username and password for most every site they visit — a habit that puts their personal data in jeopardy, as well as the schools'.

10. Participating in chat rooms or social networking sites

The very same parents who frantically try to keep their kids off of MySpace are now flocking to business social networking sites like LinkedIn, either from home or at the school. They join a colleague's "network" on LinkedIn, post messages, and maintain their own presence on the site. That's much safer than MySpace, because it's just like a professional organization, right?

Wrong. Social networking sites are a social engineer's dream come true. The bad guys use information on social networking sites to exploit you and your network.