



10 Most Dangerous Things Users Do Online

By The Staff of Dark Reading

URL: <http://www.schoolcio.com/story/showArticle.jhtml?articleID=193401932>

Courtesy of Dark Reading

End users — god bless ‘em. You can’t live with ‘em — but without them, you wouldn’t have a job. They’re the reason you have an IT infrastructure; they’re also the single greatest threat to the security of that infrastructure.

Because, in the end, most users have no idea how dangerous their online behavior is.

No matter how many times they train them, no matter how many classes they hold, most IT 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.

Wouldn’t it be nice if you could give end users a list of the most dangerous things they do online every day, and then tell them why those activities are particularly risky?

We thought so, too. The following is our list of "The Ten Most Dangerous Things Users Do Online," along with some explanation of the risks — and solutions — associated with each. This list was generated directly from input we’ve received from IT people like you, and is arranged in descending order of danger, based on votes received from the experts and analysts who make up *Dark Reading*’s editorial advisory board.

Stick this up on the door to your office. Better yet, stick it up on the company bulletin board — or post it directly to each of your users. If it keeps one user from making a big mistake, then we’ll have done our job — and so will you.

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 IT department, are there any users *left* out there who don’t know they aren’t supposed to open email attachments from strangers?

Apparently, there are. IT managers, consultants, and other experts maintain that of all the dangerous things corporate end users do, opening email attachments is still the most potentially damaging. 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. And because these attachments usually contain applications or executable files, they have the greatest potential to instigate the complete takeover — or destruction — of an

enterprise PC.

But shouldn't end users know this by now? An August survey by security software vendor Finjan offers an interesting perspective. In a straw poll of 142 U.K. office workers, Finjan found that 93 percent of respondents knew that attachments and links found in email messages could contain spyware or other forms of malicious code embedded in them.

The problem isn't that users don't know the risks — it's that they can't help themselves, Finjan said. In the survey, 86 percent of the workers admitted they open attachments and click on links without being sure if it's safe to do so. And despite frequent warnings, 76 percent of those surveyed said they routinely open what they assume to be viral marketing files, such as funny videos, jokes, or Websites.

"It's still the most dangerous thing end users do," says Richard Stiennon, founder of IT-Harvest, an IT consulting firm.

2. Installing unauthorized applications

What do you mean, "no IM?"

If you're like many organizations today, prohibiting instant messaging is out of the question. IM is rapidly becoming a standard corporate 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.

"IM is too useful to completely restrict. If you try to lock it down, but don't provide any outlet for employees to stay in touch with the outside world, users will find a way around your security policy," says Thomas Ptacek, a researcher with Matasano Security. "It's 2006. Your users are going to use IM."

IM isn't the only peer-to-peer app your users may be installing on their desktops. There's Kazaa and other free file-sharing utilities that let users share documents, software, and music. But this freedom has its cost. "These applications can increasingly be the source of new viruses," says Rob Enderle, principal analyst with the Enderle Group, an IT consultancy.

And like other unauthorized or unregulated communication, P2P apps create the risk of bad stuff coming in and sensitive corporate or personal stuff going out.

It's safest to standardize on one of the popular IM platforms, such as AIM and MSN, for instance, says Ptacek. "The only question is whether you're going to be able to monitor and control it or not."

The best defense is to ensure users have only user — not admin — privileges on their machines, says Daniel Peck, a security researcher with SecureWorks. And have a written corporate policy about what users can and can't do with these apps.

"And never install programs unless you know what they do, whether they are 'comm' programs or otherwise," says Gary McGraw, CTO of Cigital.

Your desktop firewalls can block specific ports, for instance, and a host-based IPS can also help you lock down your desktops. "But that's not foolproof," warns Peck. If your organization can't live without instant messaging, you can require IM sessions to be encrypted, he says.

3. Turning off or disabling automated security tools

It still happens: A user, frustrated by the slow performance of an ISP link or the constant exclusion of specific types of files, finds a way to turn off the firewall on his remote PC — or even at a branch office. Then, as if that's not bad enough, he "forgets" to turn the firewall back on, leaving that site open to all sorts of attacks until someone from IT finally recognizes the problem and reactivates the barrier.

And it isn't just firewalls: 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.

The disabling of carefully-evaluated, state-of-the-art security technology might be the most dangerous thing that users regularly do, according to the Enderle Group's Enderle. "This is what keeps many of us [IT and security professionals] up at night," he says. "Security applications take some overhead and may lower performance [of the end station]. Folks will turn them off as a result."

Cigital's McGraw agrees. "Sometimes you just have to postpone the old monolithic virus scan so you can get some work done," he notes. "There's always a tradeoff — make sure you make the right one."

Most enterprise firewalls and antivirus applications now contain configuration options that enable IT to eliminate the "turn it off" option from the user's desktop, McGraw observes. In many cases, it may be better to force the user to accept a patch or a slow ISP connection — and deal with the complaints — than to leave the company's systems open to remote attack, experts say.

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 training lately, and still labor under the illusion that only email attachments can contain malware.

Many experts now believe that HTML mail poses a threat that may eventually be as serious as the traditional email attachment. HTML text — and increasingly, images — can be infected with spyware, and in some cases, executable code. In July, experts at iDefense Labs, the security research arm of Verisign, discovered a new, relatively simple method of embedding shell code into commonly-loaded Web images, such as computer graphics, online photos, or PDF documents. (See [Lethal Shell Game](#).)

HTML files may contain Java Scripts, ActiveX controls, or macros that can allow an attacker to gain control of a PC or turn into a botnet zombie, noted Finjan, in a White Paper issued last month. "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," the company said.

In a study of the Web surfing habits of some 15,000 business users, Finjan found that about 6.9 percent of HTML traffic contained at least one content type that violated the security policy of the enterprise involved. Studies such as these have caused some enterprises to restrict the use of HTML email, or even disallow it altogether.

"There is plenty of active-content spam out there, and phishers use it, too," says Cigital's McGraw. "When in doubt, delete it without looking at it. If it's important, real mail, the sender will try again — or maybe even pick up the phone."

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

One of the oldest abuses of corporate 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.

Most companies today have established that such content, even when technically legal for consumers, could create a hostile working environment for employees, subjecting the company to legal or punitive action. Any human resources department will tell you that these pursuits are a major no-no, and most IT professionals will tell you that they have deployed some sort of content filter to restrict access to objectionable content.

However, the problem still runs rampant in some organizations. In fact, an investigation of the U.S. Department of the Interior published last month turned up some alarming data regarding the online surfing habits of its 80,000 employees.

In a study of one week's worth of computer logs, the U.S. Office of the Inspector General (OIG) discovered over one million log entries in which 7,763 DOI computer users spent more than 2,004 hours accessing game and auction sites. Extrapolated over the course of a year, these shopping and gaming binges could account for 104,221 hours of lost productivity — more than \$2,027,887 in lost costs, the OIG said.

The OIG found that a significant number of employees were accessing pornographic sites, many for periods of 30 minutes to an hour. Four employees were found to have downloaded egregious volumes of pornography, including child pornography, and each was prosecuted and sentenced for anywhere from 10 months to eight years in jail.

The DOI had implemented Website monitoring and blocking software, but users were still able to get around it, the OIG said. In a final spot check of the DOI systems in August, OIG investigators were able to access both pornographic and gambling sites on three of the department's four main computer systems, despite the presence of content filtering and blocking tools.

Online gambling and pornographic sites also are "becoming a frequent source of infection via drive-by downloads and zero-day exploits," observes Richard Stiennon, president of IT-Harvest.

6. Giving out passwords, tokens, or smart cards

The password problem is as old as computers themselves. Despite years of trying, however, no one has come up with a workable solution.

In a study published just this week by global research firms Nucleus Research and KnowledgeStorm, companies' attempts to tighten IT security by regularly changing and increasing the complexity of passwords is having no impact on security.

Despite years of IT warnings to the contrary, about one in three people still write down their computer passwords somewhere near the machine, either on a piece of paper or in a text file on a PC or mobile device, the researchers said.

"This is really a lot like Mom and Dad buying a great new security system for the house, and Junior leaving the combination under the doormat," said David O'Connell, senior analyst at Nucleus Research, in a published interview. "Passwords are high maintenance. People forget them, people lose them, they have to be reset."

Some experts also say that employees can be too trusting of acquaintances, colleagues, and family members who may "borrow" their passwords or authentication tokens, exposing them even more broadly to loss or theft. This is a particular risk among telecommuters or road warriors who may give out their passwords to

help a friend or relative. "You might trust the employee, but you have to draw the line at friends and family," says one expert.

The researchers at Nucleus Research and KnowledgeStorm suggested that enterprises should look to increasingly improving authentication technologies, such as single sign-on and biometrics, as potential answers to the age-old problem of password management. Online payment vendors Pay By Touch and UPEK earlier this month unveiled a finger-sensor payment service, TrueMe, which lets users access account information through a biometric fingerprint scanner. (See [Power Pay](#).)

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 and Mozilla, which have been busy patching new vulnerabilities the past few months. If your organization gives users free reign to surf the Web during or after business hours from the corporate network, beware.

In addition to the well-documented cross-site scripting (XSS) vulnerabilities floating around, there's also a lot of adware and spyware. (See [Hackers Reveal Vulnerable Websites](#).) You shouldn't put it past that 20-something intern to download some free music, for instance, and inadvertently contract some malware as a result.

Even if your corporate policy restricts Web access, the 20-somethings may not honor it. "This is something that young employees, bored security guards, and interns are more likely to do," says the Enderle Group's Enderle. "It's an attractive nuisance, and one of the reasons for a proxy server."

Internet Explorer 7.0, which was released by Microsoft yesterday, and the new upcoming Firefox 2.0 are expected to help browser security — at least until attackers start cracking them. But that may be wishful thinking: IE7's first bug was reported just hours after it went live last night, although Microsoft says the issue is a component in Outlook Express rather than in IE7.

"Attackers have started to compromise enterprises through the use of browser-based and other client-side vulnerabilities," says David Goldsmith, president of Matasano Security. "This also applies to home users who are becoming increasingly more security-savvy. Hopefully, the releases of Internet Explorer 7.0 and Firefox 2.0 will make it even more challenging for attackers to compromise the browser."

So if you're going to restrict Web access, how do you determine what sites you can trust or not? "If you're really paranoid, surf with active content disabled, use Opera or Firefox, and run your browser with very little permission," says Cigital's McGraw.

8. Attaching to an unknown, untrustworthy WiFi network

There's nothing more soothing than a good cup of java (lower-case) 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.

Your users are even more at risk if their wireless card uses the Wireless Access Protocol (WAP), which is notoriously simple to hack. A hacker can use a sniffer and grab your corporate user name and password, for instance, or infect you with a worm, says Daniel Peck, a security researcher with SecureWorks.

Even if they're only sipping coffee and working offline, an attacker could use your employee's wireless card to access his machine — and eventually, your corporate network.

It's tempting for a user on the road to jump on the closest WiFi connection they pick up while waiting at the airport or some other public place. "There is no way of ensuring that the networks they connect to aren't run by a malicious attacker," says Matasano Security's Goldsmith. "While the unsuspecting user surfs the Web, an attacker could be using a man-in-the-middle attack to monitor their traffic — or even worse, use a client side attack toolkit to compromise their machine."

A personal firewall can help, says the Enderle Group's Enderle — as long as your users keep it turned on, that is.

"Attach away. Just tunnel through with SSH or a VPN client," says Cigital's McGraw. "Also be aware of low-level attacks, and don't do anything too sensitive."

But the only way to ensure that your users won't get hacked via WiFi is to have them disable their wireless card altogether while they work from public places, says Matasano Security's Ptacek. "The safest reasonable attitude right now is that even browsing available wireless networks is risky."

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 corporate data.

"Most Websites handling sensitive info use SSL to protect the data in transit — check for that," says Cigital's McGraw.

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 company's.

And even a trusted site can have an XSS exploit embedded in it. All it takes is for a user to read a message on a bulletin board post that contains malware, and an attacker could gain control of the user's browser session.

Remote sessions should be encrypted using SSL. But SSL isn't foolproof — it has its own litany of problems and weaknesses, such as its susceptibility to man-in-the-middle attacks and keystroke loggers. "SSL has had some issues, but it's the best thing out there," says SecureWorks' Peck.

But the bottom line is that consumers are more likely to enter sensitive data into Web scripts or registration pages than enterprise users, says the Enderle Group's Enderle. "Employees seldom have the opportunity to do this," he says. "Of course, we probably

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 office. 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 biggest security challenges businesses face with business social networking like LinkedIn is the sheer

amount of information that a social engineer can learn by doing simple searches," says Matasano Security's Goldsmith. "Attackers can find out who your business partners, vendors, and clients are simply by viewing your shared connections."

There's simply no way for LinkedIn and other sites to validate a member's employment record, so an attacker can claim to work at Matasano and find out which current and past employees are on the site. "Services like LinkedIn try to guard sensitive employment information by restricting it to colleagues — you have to have worked with Dave Goldsmith before to be able to click on him and see his work history, or have him come up in a search for 'Matasano,'" says Matasano's Ptacek. "But anyone can sign up to LinkedIn and claim to have worked for Matasano."

Users can also inadvertently leak sensitive company data in a message board post with a buddy, for instance. It may reach eyes for which it wasn't intended, or they may not realize that chatting about what they're doing at work today may lead to a corporate data breach. "It's different than having drinks with a buddy after work," says SecureWorks' Peck.

Aside from a chatty user, a browser can also be a weak link. "ActiveX controls and their browser can be used by an attacker to get into the corporate network," Peck says. "There are a lot of Web app vulnerabilities we've seen."

Even if you have a "closed circle," that doesn't mean you don't touch the outside world. Just clicking onto the site of a buddy's buddy can get you into security trouble. "Every subpage you go to in LinkedIn or MySpace is like going to a whole different Website," Peck says. "It's most risky when you're going to the sites of people you don't know."

Aside from the social engineering threat, there's also the very real threat of getting infected with XSS, keyloggers, worms, and spyware (just ask MySpace users). "There's going to be vulnerabilities in the software," Peck says.

If an enterprise allows access to social networking sites, it must ensure that users are wary of who they're communicating with and what type of sensitive information they may be exposing. The bad news is you may not know until it's too late.

"You should assume that anything you post to a social networking site is public," says Matasano's Ptacek.

— The Staff of [Dark Reading](#)

- [Finjan Software Inc.](#)
- [Microsoft Corp.](#) (Nasdaq: [MSFT](#) - [message board](#))
- [Mozilla](#)
- [SecureWorks Inc.](#)

© School CIO