Avoiding the Dangers of Web Browsing

By Lawrence T. Levine

There is a proverb in consulting that warns against celebrating after solving your No. 1 problem, because at that instant, your No. 2 problem gets promoted, and you're back where you started.

Similarly, bankers should resist the urge to relax after implementing a firewall to fortify the network perimeter. Once it is secured and outsiders are kept at bay, the next biggest problem—attacks coming from inside the bank—becomes the primary threat.

It's not that employees are suddenly untrustworthy. Rather, the problem is that a common activity formerly considered benign—Internet Web browsing—has become highly risky.

Understanding the Problem

Unrestricted Web browsing brings with it some obvious concerns, including lost productivity, bandwidth hogging by streaming media (such as Internet radio and rich media advertisements), and the presence of content that may be construed as creating a hostile work environment.

Employees may also be using Web access to subvert corporate usage polices. For example, many personal e-mail accounts can be accessed through the Web, and these e-mails can include attachments that are invisible to the corporate and desktop antivirus software.

It gets worse. Just by browsing certain Web sites, malicious software (or "malware") can be automatically downloaded and installed on an employee's machine. This type of software includes adware, spyware, ActiveX components, and keystroke loggers. In their mildest form, these programs can take over a user's home page and present a flurry of pop-up ads. More insidious versions can capture keystrokes (such as logon credentials, passwords, and Social Security numbers) and transmit that information outside the bank's network to a third party.

The most popular Web browser in use is Micosoft's Internet Explorer. Some users are not even aware that they have a choice among World Wide Web viewers, with options such as Netscape, FireFox, Mozilla, and Opera. Among banks, the use of Internet Explorer is probably even higher than among the general population, because many core processors require it to use built-in banking applications.

The popularity of Internet Explorer is regrettable, because its design makes it the most prone to rogue installation of malware. The reason is that Microsoft integrated functions into Internet Explorer that make it easier to install and run software from within the Web viewer. This was done for competitive reasons, but the net result was that this feature has become an Achilles' Heel.

Authors of viruses and trojans have leveraged some of Internet Explorer's operating system integration to get their malware on users' machines. Other avenues of infection have exploited bugs in Internet Explorer, such as a recent vulnerability that is triggered by the display of photos on a Web page. Users do not have to click anything; just browsing a site with hacked images could infect them.

Steps for Avoidance

In most cases, victims of these browser exploits could have saved themselves if they had simply stayed out of "bad neighborhoods" on the Web. Some banks have responded to this by configuring firewalls (or Web proxies) to limit access to an explicit list of permissible sites. Whitelisting, as this practice is known, works—but it requires frequent updates, and can often be an impediment to business when site access is necessary for a non-listed location.

A more flexible approach is the use of a Web content filter system. A Web content filter acts as a go-between for your browser and the Web. When a user enters a Web address, or clicks a link on a page, the

> A common activity formerly considered benign—Internet Web browsing—has become highly risky.

request is sent to the Web content filter system, where it checks an internal database of Web sites to see whether the target site is permissible. Blocked requests are dropped, and the user is presented with an "Access Denied" page.

Web content filter systems break the Web down into categories (such as shopping, games, gambling, sports, and adult), enabling administrators to granularly define categories that will be blocked. Further, group policies can be created that allow, for example, tellers to see one class of sites, and management another. However, this stratified approach can introduce another common problem.

In many banks, it is not the line employees who are bringing in malware, but rather the managers, who are often reluctant to restrict their own access to the Internet. Bank information technology staff often know this is a problem, but may be afraid to confront management.

Because infections can occur without any specific action on the browser's part, bank managers need to face the reality that their Web browsing must be reined in. They must do their recreational surfing at home, and not introduce risk into their institution. For the safety and security of the bank, unrestricted use of the Web must now come to an end.

All views expressed are solely those of the author. Lawrence T. Levine is managing director and co-founder of SecurePipe Inc., an ACB Business Partner.

Since 1996, SecurePipe has been delivering managed network security services to financial institutions. Hundreds of banks depend on SecurePipe to protect data, reduce the cost and complexity of security monitoring and management, and improve their regulatory compliance.

The ACB/SecurePipe alliance offers managed security solutions at a significant discount for ACB members. For information, contact ACB's Sam Lisker at (202) 857-5081 or slisker@acbankers.org.

ACB Business Partners offers a complete menu of business solutions in mortgage, technology and payments, and financial and capital markets. Visit www.AmericasCommunityBankers.com/Partners *to learn more.*

Keeping It Safe

Six recommendations for controlling the risks posed by unrestricted Web browsing

1. Create a strict Web usage policy to supplement the bank's acceptable use policy.

2. If practical, consider an alternative to Internet Explorer. FireFox is not immune to exploits, but historically, bugs have been acknowledged and fixed more quickly than those in Internet Explorer.

3. Restrict browsing by implementing a Web content filter; if reasonable, consider a Whitelist configuration.

4. Keep a log of all Web usage. Reports can be used to discover violators, both by content and volume. Documentation may also be legally required in some disciplinary situations.

5. Implement an intrusion detection system to catch malware as it arrives. Even known reputable Web sites can be hacked and caused to deliver an ugly payload. An intrusion detection system is the best method to detect the installation of rogue software, giving you time to speedily contain any damage.

6. When vendors or visitors must be provided with Internet access, segregate this uncontrolled traffic by creating a DMZ, or buffer area, on your firewall that will limit their ability to access your internal network.