Securing Consumer-based Web Sites

by Douglas D. Weinberg

For many healthcare providers, the Web does not currently play a significant part in their marketing or business strategy. That is about to change as healthcare providers become increasingly aware of what other industries have known for some time—using the Web to communicate with consumers creates significant opportunities for consumers and providers alike.

For consumers, the Web offers the prospect of cheaper, more convenient, and more flexible healthcare options. Healthcare providers can use the Web to deliver and gather information and to provide treatment options less expensively. Well-designed Web sites can also boost customer loyalty, potentially leading to more business. A combination of consumer demand, regulatory changes, and cost incentives will transform the Web from an optional marketing tool to a strategic necessity. And, as has happened in other industries, smart first movers will reap the benefits sooner.

Web-based technology also brings security challenges. As consumers begin to access confidential information and interact with providers over the Web, security needs will increase substantially. Many providers will look to their experiences in implementing HIPAA to guide their Web security views. HIPAA provides excellent guidance, but some lessons need to be adapted to deal with the unique challenges of new users, new technologies, and new security threats.

Web Security: What's Different?

Consumers have different needs and capabilities than traditional users, and this will require many institutions to adapt their security practices. The main users of provider systems and data have been a limited number of identifiable and relatively sophisticated institutional users. This group is comprised mainly of employees, consultants, affiliates, payers, and vendors. These users had their own IT departments to ensure system security. Institutional users could also be carefully screened and monitored, assigned to work only on designated systems, and be trained in the proper use of the systems.

On the other hand, consumers have a different profile. For one thing there are more of them, therefore methods to authenticate or identify them need to be relatively inexpensive and largely automated. Special security hardware such as secure IDs or virtual private networks is usually impractical because of the cost. User IDs and passwords need to be generated with minimal human intervention.

Furthermore, consumers as a group are relatively unsophisticated about security. They don't have IT departments, and their approach to security is piecemeal at best. Some experts now say that poorly protected home PCs pose the biggest threat to computer networks for businesses and governments. Thus, provider systems must limit consumer interactions to those which they can sufficiently protect. In addition, security schemes for consumers have to be simple, even transparent. Consumers don't have the resources or patience to implement sophisticated security schemes. Therefore security tools such as encryption should be automatic, as on most credit card sites.

Different Technologies and Threats

Another reason that Web security will need some adaptation is new technology. Over the past few years there has been a proliferation of wireless technologies, including advanced cell phones, Bluetooth, connected PDAs, wireless hotspots, wireless DSL, and tablet PCs. These technologies offer new ways to get information to and from consumers, but they can also pose new security threats.

Technology advancement has also produced new and cheaper methods of protecting assets, ranging from free firewalls to fingerprint readers built into PCs. As the cost of similar technologies decreases, they may become increasingly viable methods to use with consumers.

There are other new types of threats. Spyware, phishing, and pharming are examples of threats that have grown in recent years. Some software in these categories, like certain types of spyware, can have legitimate uses, making it harder to screen out.

Spyware

The fastest growing category of security threats is spyware. By one estimate, 20,000 new spyware programs were identified last year. Spyware collects personal information from a computer without the user's knowledge or consent and sends it to third parties. The information collected ranges from the Web sites visited to passwords and credit card numbers. In contrast to viruses, which usually seek to create dramatic (and terrible) effects, spyware usually works in the background. Spyware infects two-thirds of user computers, often without the user's knowledge. It usually accompanies downloads of music, games, or other files, usually from unfamiliar sites. Users often unknowingly consent to the installation of spyware by accepting a license agreement containing consent.

By using the computer to collect and send information, spyware slows performance, in some cases significantly. More importantly, spyware disseminates private data without consent. Two obvious dangers for healthcare providers are having user IDs and passwords to their sites stolen and having confidential information unknowingly disseminated.

There are numerous effective antispyware programs, several of them free. In addition, applying security patches and program patches routinely and keeping a browser's security on a high level can help significantly reduce the incidence of spyware.

Mobile Technology

If it weren't bad enough that personal computers are vulnerable, hackers have begun to target cell phones, handheld PCs, PDAs, and other mobile technology. There have been a growing number of reports of these attacks in recent months. The main way to contract these viruses is to download files such as new ring tones, pictures, videos, e-mail messages, or programs.

The good news is that many experts believe the current risk is limited. One reason is mobile devices have diverse operating systems. A virus that exploits a security flaw in one system's operating system often cannot easily propagate to or damage another device with a different operating system. In addition, the software running traditional cell phones is not easy to attack. However, as users increasingly rely on smart phones with e-mail, instant messaging, and Web-browsing capabilities, they will become more vulnerable to attack. Vulnerability will also increase as viruses become more sophisticated and if a single operating system becomes dominant on mobile devices.

The case of mobile technology provides a good example of how, by better understanding security risks, organizations can put their resources where they are most needed. The risk of having data on a cell phone or PDA lost or stolen by a virus or other software is relatively low. By contrast, the risk of such loss is much greater from the theft or loss of the device. Thus, the best way to protect against data loss is to encourage users to treat portable devices as they would a purse or wallet and to have them use a password to secure access to their devices.

Bluetooth

Bluetooth technology allows data transfer between nearby devices, usually within 30 feet of each other. Examples include transferring contact information from a cell phone to a desktop computers and moving pictures from a digital camera to a printer. One of the most popular Bluetooth applications is a wireless earpiece enabling hands-free talk on cell phones.

The main security risk with Bluetooth devices is that they can unintentionally contract and transmit viruses. If an uninfected Bluetooth device is detected by an infected Bluetooth device running the same operating system, the uninfected device could get the virus. An easy way to reduce this risk is to disable Bluetooth or set the device to nondiscoverable mode when not transmitting files.

Phishing and Pharming

Phishing seeks to get users to disclose confidential information under false pretenses. Con artists send blast e-mails that appear to be from popular or trusted sites, such as banks and credit card companies. The e-mail messages, related Web sites, and pop-

up windows appear legitimate enough that people respond to requests for credit card numbers, passwords, or account information. The phisher then uses the information on the actual site to obtain information, steal identities, or conduct fraudulent transactions. Banks and other financial institutions are common targets.

In pharming, hackers redirect Internet traffic from a legitimate Web site to a spoof site in order to trick users into entering their user names and passwords. Pharming is more sinister than phishing because it avoids the need to coax users into responding to junk e-mail alerts. Users are redirected to a false site without participation or knowledge. These sites can be sophisticated and hard to detect.

To counter phishing attacks, users should be suspect of any e-mail that requires them to provide confidential information over the Web or phone. Pharming is much harder to combat since hackers hijack the central database that controls Web site addresses. If pharming grows as a threat, banks and similar institutions (such as healthcare providers) could adopt such strategies as a two-step authentication. Fortunately, there have been few documented pharming attacks. Furthermore, government and business have a strong interest in preventing these attacks to preserve the integrity of the Web.

Why Do I Need to Know This?

You may ask why you need to know about Web security issues—the IT department handles them. However, if you are going to help shape your facility's policy on consumer access to confidential information online, you need to know the security risks involved because they will affect what you do and how. You do not need to be an expert, but you should know the risks and how to spot them. Moreover, despite the formidable capabilities of many IT departments, there are many cases where spyware, viruses, and other threats have sat on PCs for a long time, slowing performance but never removed because no one spotted them.

Even if your institution screened out all potential threats, you still want to help your consumers avoid them. It does not help your facility if consumers cannot successfully access your site or if confidential information you provide to consumers is snatched and disseminated by spyware. Finally, on a personal level, you are a consumer, too, and knowing about security directly affects you.

Web technology will provide an increasingly compelling source for providers to connect with consumers, but it will raise new security concerns. Understanding these concerns and how they may differ from issues already encountered will give you a big head start in moving toward an effective consumer-based Web strategy.

Douglas D. Weinberg *(doug@cobius.com) is the president of Cobius Healthcare Solutions, LLC, in Northbrook, IL.*

Article citation:
Weinberg, Douglas D. "Securing Consumer-based Web Sites." *Journal of AHIMA* 76, no.10 (November/December 2005): 58-59,64.