Think Your Network is Safe from Data-Stealing Malware?

THINK AGAIN!

By Sandi Hardmeier

HOW SAFE IS YOUR PRACTICE'S CRITICAL BUSINESS INFRASTRUCTURE AND COMPANY DATA? Maintaining effective defences against constantly changing security threats in today's internet-driven world has become ever more complicated, given the sophisticated dangers that we face today.

Thankfully our employees are far more 'internet savvy' than they were a few years ago (the 'Iloveyou' virus of 2000 was a warning not to open attachments promising to be declarations of love), but now is not the time to relax our guard. Social engineering is still one of the most effective tools in the internet criminal's arsenal, and it does not have to be highly accurate in its approach – just plausible.

Imagine this. Your company recently purchased 40 new Hewlett Packard desktop computers. Your accounts department receives an email, apparently from HP, with an invoice attached. The email has a link for querying or disputing the invoice.

Would your employee open the attachment? If the invoice listed 60 computers instead of 40, or an invoice had already been received, would your employee click on the link to dispute the invoice?

This incident occurred less than a year ago and, yes, both the email and invoice were fake. The employee opened the attachment, and clicked on the link to visit the website and dispute the invoice.

Luckily the attachment did not contain a virus, and the website was a basic phishing site, but if the same thing happened today, you can bet that the invoice would take advantage of a security vulnerability, and the website would contain malicious code designed to infect the visitor's computer with, at best, fake security software or, at worst, a key logger or other spying software designed to quietly steal keystrokes and/or sensitive business intelligence.

Dangers posed by cyber crime can appear anywhere. For example, the first eight months of 2008 were the glory days of a hacker trick called 'SQL injection'. At its peak, we had to treat any website with a search field, or a field that accepted user input (for example, 'contact us' forms, 'leave a comment' forms and the like), as a potential danger. Some very big names were caught unawares and hundreds of thousands – if not millions – of people were exposed to danger. Some websites continue to be a risk to visitors, despite attempts by the security community to warn the site owners.

'Malvertising' is another danger that has appeared during the past few years. In November 2007, Sensis was tricked into accepting malicious advertisements that were displayed on whitepages.com.au, yellowpages.com.au, tradingpost.com.au and other Sensis properties. The ads were designed to take visitors away from Sensis-controlled pages to other sites; web pages that were designed to infect computers with fake security software. Soon after the Sensis incident, mlb.com was tricked into displaying a malvertisement that loaded a hard porn website, complete with streaming video and audio.

The most important message here is to realise that the modern-day internet criminal has developed exquisitely sophisticated ways to target your employees (and your practice), whether via social engineering or attacking the sites and services that your employees use. 'Knowledge is power'; once we know what is happening and understand why, we are better-placed to respond. Future articles will discuss not only what is happening, and why, but also the implications for our businesses.

Welcome to the darker side of the internet!

Sandi Hardmeier is a journalist who has been awarded the Microsoft MVP every year since 1999.
EMAIL **columnfeedback@mvps.org**