Securing the Weakest Link: Educate End Users about Cyber Risks

Nearly every day you read about a new malicious attack on computer networks of vital businesses around the world, and the attacks do not seem to be slowing down.

According to reports, malware volume skyrocketed in 2016 - more than 800 percent when compared to 2015 – and that number is continuing to rise.

The most recent, the WannaCry ransomware attack, targeted computers running Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin currency. The attack reportedly locked hundreds of thousands of computers in more than 150 countries and demanded a $300 payment to restore the encrypted files.

Another attack, the Hancitor malicious downloader, worked its way into networks using a variety of fake emails from what looks like familiar senders such as FedEx, USPS and Google. These emails appear to be authentic, making it more likely that users will click a link within the body of the email. Doing so, however, will download an exploit that allows cybercrooks to take control of the infected machine.

“Attackers are getting more sophisticated, creating very realistic emails that can easily catch end users off-guard,” said AppRiver security analyst David Pickett. “It pays to read carefully, looking for misspellings and typos that most businesses, government agencies, and media outlets simply don’t make.

Pickett added: “As a general rule, don’t click on a link within the email. Where possible, go directly to the site and find the information there. If you can’t, there’s a good chance the email link was malicious.”

So what else can businesses do to protect themselves?

Aside from a mulit-layered security approach, businesses should have a secure backup process in place. Should they be infected, a backup allows them to wipe the affected device and reload their information. Usual.

Another crucial step is education for all levels of staff.

Often it is a company’s last line of defense – the employees – who accidentally unleash a malicious attack.

It is worth an employer’s time to educate employees on how to not fall prey to a savvy hacker because it just might save the company from costly attacks and hours of headaches. And as a trusted advisor, you’re in the best position to help.

“Channel partners and network admins consistently tell us that their biggest security concern is their own or customer employees downloading malware,” said Justin Gilbert, AppRiver channel sales manager. “It is that point where education can be even more critical than technology in preventing breaches.”

Securing the Weakest Link: Educate End Users about Cyber Risks

appriver® Email & Web Security Experts™

Here are 5 simple steps you can teach end users that will help keep hackers from wreaking havoc on your systems:

1. ***Assume all file attachments are dangerous:*** Dangerous attacks often utilize common file types users are used to seeing - .doc, .xls and .pdf, etc. While not every file extension can launch a malicious attack, users should treat file extensions with a healthy dose of skepticism – especially if the files were received unsolicited.

2. ***Stay alert for phishing emails:*** Only click web links within emails you absolutely are sure are authentic. Phishing emails typically come with typos and impersonal greetings such as “Dear Customer” or “Dear Sir/Madam.” Be wary of threats and urgent deadlines as these often are characters of phishing scams.

3. ***Update system and software patches regularly:*** Security researchers have shown that installing system and software updates is the best defense against the most common viruses and malware online, particularly for computers running Windows. Software makers often release updates to address specific security threats that have come to their attention. By downloading and installing the system and software updates, you patch the vulnerabilities that virus writers rely on to infect your computer.

4. ***Be careful using public WiFi:*** Most businesses that provide public WiFi tend to have lax or nonexistent security – leaving the network and your computer vulnerable to hackers.

5. ***Use complex and lengthy passwords:*** To make it harder for someone to guess your password, use a combination of letters, numbers and symbols. Do not use the same password for multiple accounts.

If you’d like to share this information with your customers and their end users, AppRiver has made it easy with this downloadable poster you can print and distribute.