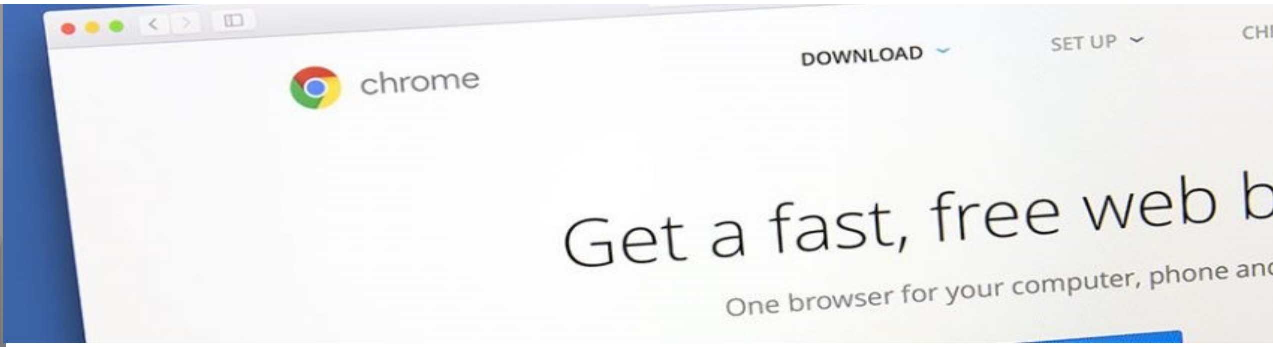
E-SAFE TECHNOLOGIES

E-NEWS

www.E-Safetech.om | 1-412-944-2402 |

May
2017

In this issue...



Get a fast, free web b

One browser for your computer, phone and

The most advanced Gmail phishing scam yet

As the technology that recognizes and thwarts malware becomes more advanced, hackers are finding it much easier to trick overly trusting humans to do their dirty work for them. Known as social engineering, it's a dangerous trend that is becoming increasingly prevalent. Read on to educate yourself on how to avoid the most recent scam and those that came before it.

Broadly defined, "phishing" is any form of fraud in which an attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels.

These messages prey on users who click links, images and buttons without thoroughly investigating where they lead to. Sometimes the scam is as simple as an image with a government emblem on it that links to a website containing malware. Just hovering your mouse over the image would be enough to see through it. But some phishing schemes are far more difficult to recognize.

The Google Defender scam

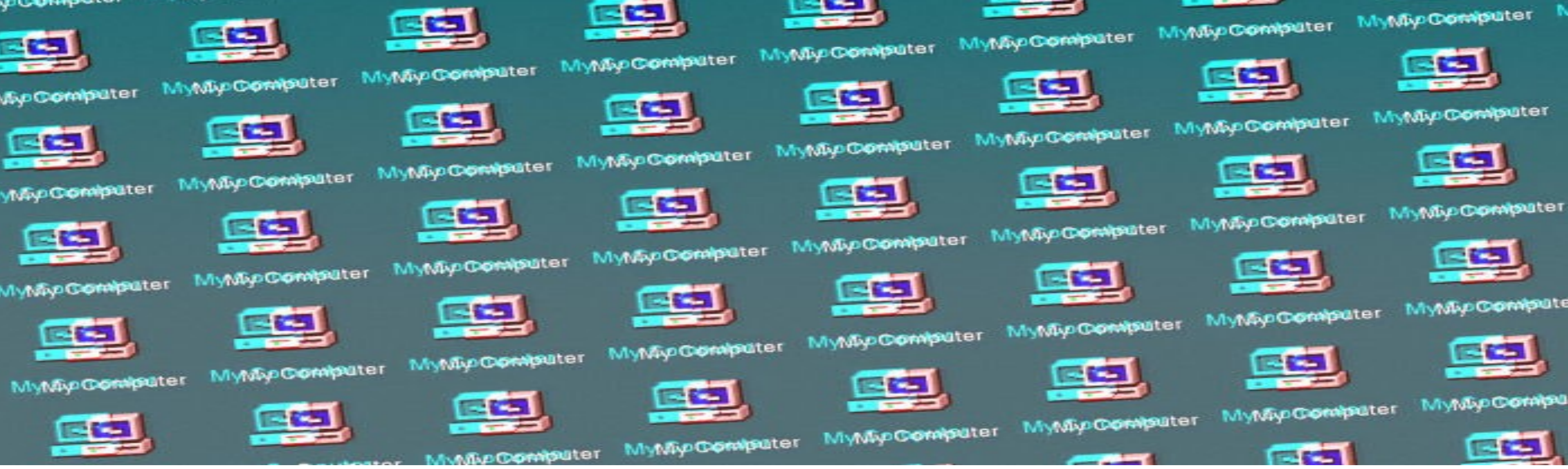
Recently, an email spread to millions of Gmail accounts that almost perfectly imitated a message from Google. The text read:

“Our security system detected several unexpected sign-in attempts on your account. To improve your account safety use our new official application “Google Defender”.

Below that was a button to “Install Google Defender”. What made this scheme so hard to detect is that the button actually links to a totally legitimate site...within Google's own framework. When third-party app developers create Gmail integrations, Google directs users to an in-house security page that essentially says, “By clicking this you are giving Google Defender access to your entire inbox. Are you sure you want to do this?”

Even to wary users, the original message looks like it came from Google. And the link took them to a legitimate Google security page -- anyone could have fallen for it. The Gmail team immediately began assuring users that they were aware of the scam and working on eradicating it and any potential copycats.

There's no happy ending to this story. Although vendors and cybersecurity experts were able to respond to the crisis on the same day it was released, millions of accounts were still affected. The best way to prepare your business is with thorough employee training and disaster recovery plans that are prepared to respond to a breach. To find out how we can protect your business, call today.



For Windows Pros, The WannaCry Ransomware Mess Was All Too Predictable

April was known as "Ransom Awareness' month. One month later and one of the biggest ransom stories to date has occurred. In early May the WannaCry ransomware outbreak shocked the world.

The security flaw that caused May's devastating worldwide "WannaCry" ransomware attack was the worst of all types of bugs. A so-called "remote code execution" vulnerability in older versions of Microsoft Windows gave the cybercriminals behind the attack full control over infected machines. After successfully infecting a PC, the worm encrypted data files and posted a demand for ransom; it then began spreading over the corporate network, using a flaw in an old and notoriously insecure networking protocol.

To wreak their havoc, the unknown attackers behind this outbreak used a tool originally developed by the U.S. National Security Agency to break into networks belonging to hostile foreign powers. That tool was one of nine released onto the internet in April by a separate but equally mysterious group of hackers called the Shadow Brokers and weaponized in less than a month for this attack.

As shocking as the attacks have been, they were made possible by issues that the IT experts responsible for maintaining Windows systems have known about for many years–some of which involve decisions that Microsoft made in the previous century

This Type of Outbreak Has Happened Before

IT pros who've been in the business for more than 15 years have painful memories of the first decade of the 21st century, when one internet worm after another attacked PCs and corporate networks worldwide. As in the current attack, the Code Red and Nimda worms (2001) and Blaster (2003) were capable of jumping from one PC to another over a network. Microsoft responded in 2002 with a fundamental change in the way it developed Windows and other software, called Trustworthy Computing.

The Primary Victims were Running Outdated Windows Versions

PCs running the latest Windows release, Windows 10, are immune to the WannaCry worm. In March, Microsoft released a software fix for PCs running Windows 7, and network administrators who installed that update promptly were also protected from infection. PCs running Windows XP, which was originally released in 2001, were especially likely to be victimized. Microsoft ended support for Windows XP in 2014, and only large customers who pay dearly for extended support contracts get security patches.

In Some Cases Updating the Software isn't an Option

Even conscientious IT pros can face a dilemma when critical equipment such as an MRI machine is running an old operating system and the manufacturer no longer provides upgrades. Taking that expensive piece of machinery out of service isn't an option, but leaving it connected to a network introduces significant risks.

This Nightmare was Predictable and Completely Preventable

The software flaw that made this outbreak possible was in a piece of code called Server Message Block version 1 (SMBv1, for short). By internet standards, this protocol is downright ancient, dating back to the early 1990s. Microsoft began warning customers in November 2016 to stop using it and issued an even more urgent warning in March, along with software updates for Windows 7 and Windows 8. Those who didn't heed those warnings are paying the price today.

Austerity Budgets Exacerbated the Problem

Critics in the U.K. have already pointed the finger at budget cuts, including the government's decision to save roughly £5.5 million this year by not renewing a custom support agreement for its large installed base of Windows XP PCs. But IT pros worldwide say budget cuts have turned their departments into the equivalent of emergency room doctors, dealing only with the most urgent issues. Typical IT departments don't have the money to invest in infrastructure improvements as a strategic bulwark against precisely this sort of attack, and the rise of outsourced IT departments means those who are doing support tasks don't have a say in critical business decisions.

Through a happy accident, security researchers were able to disable WannaCry quickly, stopping it in its tracks within a day. But the combination of vulnerable PCs and networks, inadequate budgets, and frazzled IT departments means that it's only a matter of time until another wave arrives.

Majority of CEOs Knowingly Raise Risk Level With Their Shadow IT

Despite the increased risk shadow IT poses to security, a majority of CEOs surveyed say they are willing to take the risk, according to a survey released today.

A majority of CEOs are willing to put their organizations at risk by using shadow IT, even though they are well aware of the potential security fallout, according to a report released today by Code42, a cloud-based security company

The survey of 1205 IT and business decision makers revealed 75% of CEOs surveyed acknowledge using applications and programs not sanctioned by their IT departments, despite 91% of surveyed CEOs acknowledging this behavior could put their organization at a security risk, the study found.

When the top dog behaves in such a cavalier fashion, it can potentially set the tone for the entire organization, says Rick Orloff, chief security officer for Code42.

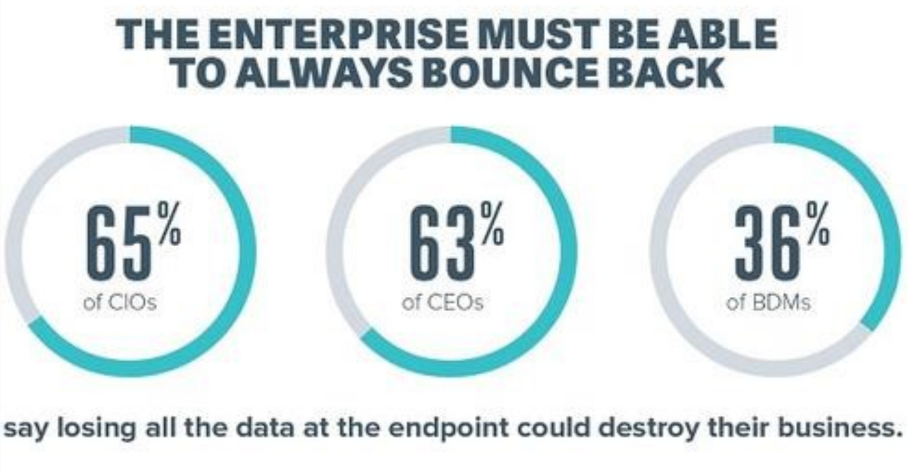
If employees see the CEO doing their own thing, it gives them a sense of entitlement and contributes to the friction with the security team and employees feel they don't have to comply with policies and best practices, Orloff says.

He added there is also an additional impact to the company.

“When CEOs behave this way, then the CISO is not reporting high enough into the organization, CISOs should ideally report into the CEO and not the CIO,” says Orloff. “I bring this up because when the CISO reports directly into the CIO, there is an air gap between the CISO and senior leadership. When you remove the air gap, then you don't have the shadow IT.”

Without the air gap, a CISO can work with the CEO to find the tools needed to do the job using existing authorized technology, or bring in the right secure tool onto the platform, Orloff explains.

Driving the behavior to use shadow IT is a desire by CEOs and other company executives to put convenience and productivity ahead of security, the study found. This long-held mantra of productivity over security is nothing new when it comes to rand-and-file workers, but for top-level management to knowingly disregard best security practices is somewhat surprising, considering that they recognize there is a risk, and that these executives themselves are increasingly held accountable for security breaches.



Although 83% of surveyed business decision makers are well-aware of the security risks that their actions pose when using shadow IT, they are nonetheless willing to take such action under these circumstances. According to the survey, respondents would:

- Use an unapproved application or program if it would improve their productivity (65%)
- Use shadow IT if it would make their lives easier (52%)

Use it because the IT department does not understand what is needed to get a job done (27%)

But the figures that surprised Orloff the most were the percentage of CEOs who knew use of shadow IT was a security risk. "I expected it to be around 35% and 40%," he says, versus the 75% and 91% figures in the survey.

The survey also found that business executives tend to be more concerned than IT security executives that a major data breach will happen in the near future. For example, while roughly half of business decision-makers and also IT leaders say they encountered a security breach in the past 18 months, of those who have not, 88% of company executives versus 50% of IT decision makers expect a breach to go public in the next 12 months, the study found.

Business decision makers expecting a public breach within the next 12 months may have more heightened concern than their IT department because they have heard about the sizable breaches hammering companies over the past 18 months and do not understand their own company's security footprint, says Orloff.

Although business executives and IT professionals have a gap when estimating the next breach, their differences are narrower when it comes to the likelihood their companies would face serious repercussions if they lost all their corporate data held on endpoint devices. The survey found that 90% of IT and business executives believe it could be serious to potentially fatal for their organizations, with 88% of IT executives and 83% of business decision makers finding their companies need to shore up their breach recovery abilities in the next year.

The Cloud is More Secure Than You Think

Even to this day, the perception of cloud technology suffers from a reputation for bad security. But as time goes on we're beginning to see that cloud security is almost always better than that of local area networks. So whether you're considering a cloud web server or internet-based productivity software, take a minute to learn why the cloud your best option.

Hands-on Management

Unless you have an overinflated budget, relying on local copies of data and software means IT staff are forced to spread themselves across a bevy of different technologies. For example, one or two in-house tech support employees can't become experts in one service or solution without sacrificing others. If they focus on just cybersecurity, the quality of hardware maintenance and helpdesk service are going to take a nosedive.

However, Cloud Service Providers (CSPs) benefit from economies of scale. CSPs maintain tens, sometimes thousands, of servers and can hire technicians who specialize in every subset of cloud technology.

Fewer Vulnerabilities

Cloud security isn't superior just because more technicians are watching over servers. When all the facets of your business's IT are in one place, the vulnerabilities associated with each technology get mixed together to drastically increase your risk exposure.

For example, a server sitting on the same network as workstations could be compromised by an employee downloading malware. And this exposure extends to physical security as well. The more employees you have who aren't trained in cyber security, the more likely it is that one of them will leave a server room unlocked or unsecured.

CSPs exist solely to provide their clients with cloud services. There are no untrained employees and there are significantly fewer access points to the network.

Business continuity

The same technology that allows you to access data from anywhere in the world also allows you to erect a wall between your local network and your data backups. Most modern iterations of malware are programmed to aggressively replicate themselves, and the best way to combat this is by quarantining your backups in the cloud. This is commonly referred to as data redundancy in the cybersecurity world, and nowhere is it as easy to achieve as in the cloud.

The cloud doesn't only keep your data safe from the spread of malware, it also keeps data safe from natural and manmade disasters. When data is stored in the cloud, employees will still have access to it in the event that your local workstations or servers go down.

The cloud has come a long way over the years. It's not just the security that has gotten better; customized software, platforms and half a dozen other services can be delivered via the cloud. Whatever it is you need, we can secure and manage it for you. Call us today.

E·SAFE TECHNOLOGIES