SIM2K
Adapting Technology to Your Business Needs

8•19
Information you can use

SIMformation

Phishing Scams Getting Sophisticated

Phishing scams are nothing new. In fact, we've all heard about the classic "Nigerian prince" phishing e-mails that started this whole e-mail scam nightmare. Unfortunately, phishing attacks continue to increase exponentially in volume, and are considered a serious threat to both companies and individual internet users, as they can result in devastating financial losses. In addition, phishing e-mails can be much harder to recognize than many business owners think.

Cybercriminals have resorted to increasingly sophisticated phishing strategies as of late to get recipients to open, click, and share malicious code. And these tactics are paying off handsomely. Business e-mail compromise (BEC) scams are more successful than ever, with losses reaching $2.7 billion in 2018.

Here are some common phishing trends that business owners should know about and tips for educating employees about them:

What are phishing scams?

Phishing scams typically consist of e-mails that seem harmless but are actually intended to trick users into sharing sensitive information. This can be accomplished by encouraging the user to click on a malicious link or attachment. Phishing e-mails get their name because the hackers are "fishing" for your personal information.

Most phishing e-mails appear completely legitimate, often by imitating a company's logo using high-quality graphics and including opt-out instructions. For this reason, it's quite common for recipients to be fooled, and even large companies have fallen prey to these scams.

Common phishing trends and techniques.

There are many techniques hackers use to launch a phishing attack. A few of the most common ones are:

Invoice phishing: Invoice phishing e-mails claim the recipient has an outstanding invoice from a well-known company, bank, or vendor. The e-mail instructs the recipient to click on a link to pay the invoice. But when they click on the link and access the site, the hackers steal their personal information and gain access to their bank accounts.

The virus or compromised account: Viruses and compromised accounts cause users to receive an e-mail from a third-party company claiming one of their accounts has been compromised. The email instructs the user to log in to reset their password or to download a form, fill in their personal information, and return it. However, a legitimate company would never request your personal information through email in this manner.

Payment and delivery scam: This tactic involves sending e-mails from what appears to be a legitimate vendor, asking for a user's credit card information. They typically claim your payment information needs to be updated before they will deliver your order. Be careful with these e-mails, especially if you haven't purchased anything from the vendor.

Downloads: Download scams send an e-mail instructing recipients to click on a link. These e-mails often contain hyperlinks that could download a malicious file onto the user's computer. Never click on an e-mail link unless you are absolutely sure the sender is who they claim to be.

Tips for spotting phishing emails.

Although phishing e-mails often mimic actual companies and vendors, there are ways to detect them. All small-business owners and employees should be aware of the following red flags that indicate a possible phishing e-mail:

- The email contains links or URLs that direct you to the wrong website or try to get you to access a third-party site that is separate from the email sender.
- You receive an e-mail from a company requesting sensitive information such as a social security number, bank account information, or credit card numbers. Consider these e-mails suspect and never share your personal information without checking with the company first.
- You find an unexpected e-mail in your inbox from a person, vendor, or company that you rarely or never deal with. If this happens, the safest thing to do is delete the e-mail without opening it, as there's a good chance it's a phishing e-mail.
- The e-mail has obvious errors like typos, poor grammar, or incorrect information. A legitimate e-mail from a company is very unlikely to have these kinds of errors.
- The e-mail address of the sender is incorrect, although it is close to the actual e-mail address. This is another common sign of a phishing e-mail.

Phishing scams remain a very common type of cybercrime, and can cause major financial losses to individual users and companies. And phishing e-mails are much more sophisticated these days, making them harder to detect. If you're a business owner, it's essential to be aware of phishing techniques and red flags, and to educate your employees on them. By doing so, you can help protect your company from financial losses and other serious consequences.

SIM2K can work with you to develop "best practices" for dealing with potential phishing e-mails and training staff to identify these. We also offer testing wherein we will send "suspect" e-mails to your staff and anyone opening one can be taken aside for more training on identifying scam e-mails. Call us for details.

Windows 10 Local Account

What is the difference between a Local Account and Microsoft Account in Windows 10? Microsoft, naturally, believes that a Microsoft account is in your best interests: Your preferences, password, and files are stored in the cloud and carry over to new devices, you can manage subscriptions like Xbox Live, and you also have access to various Microsoft services. A Local account is just that - your PC is configured as a "stand alone" device and any passwords, apps or Cloud-based services are not shared outside of your PC itself. Despite Microsoft's claim that a Microsoft account is best, the point is that the choice should be yours to make.

Windows 10's seetup process traditionally let you choose between either accounts. When first starting a new computer, you would be given the option to make the choice between the two. However, changes were made in what Microsoft calls the Out-of-the-Box Experience (OOBE). In 2018, Windows dropped the ability to go back and create a Local account if you had accepted the Microsoft account sign-in. The initial "choice" screen disappeared and could not be brought back. In the May 2019 Update, Microsoft seems to have relaxed its tactics. But only a small fraction of users, about 6%, appear to have access to the friendlier version as they are still on the October 2018 version.

So if you want to only go with a Local account, there are two ways to make this choice, but neither is obvious. The first way is the "official" way to opt out of entering a Microsoft account. During the Wi-Fi sign-in page, you can opt to skip it. That leads you to the page where Windows begs you to reconsider, reminding you that just a single click can save you precious time later on. Clicking "No" will take you to the local account page – though there's absolutely no helpful cue to inform you as such.

However, if you skip over that part and find yourself in the Microsoft Account sign-up page, don't despair – there's a work-around. You'll need to turn off your PC's Internet connection: Unplug the ethernet cord, disconnect the router, or turn off your laptop's WiFi using an "airplane mode" key on the keyboard (if it has one). What you're trying to do is force Windows to be unable to connect to the Internet. The goal is for the OOBE to recognize that it can't connect to the Internet, give up, throw an error message, and relent into giving you the local sign-in screen. This should take you back to the original sign-in page, only now, the only option is to create a local account.

The May update gets around this. If you choose to decline and "continue with a limited setup," you can proceed directly to the local account setup. And, if you do end up on the Microsoft account screen, there's an "Offline account" (or local account) option in the lower left-hand corner.

New Ransomware Variant

Sodinokibi ransomware, also known as Sodin and REvil, is hardly three months old, yet it has quickly become a topic of discussion among cybersecurity professionals. Sodinokibi is a ransomware-as-a-service (RaaS), and researchers believe it to be more advanced than its predecessor, GandCrab. This threat has targeted businesses and consumers equally since the beginning of May, with a spike for businesses at the start of June.

Putting a spin on an old product is a concept not unheard of in legitimate business circles. Often, spinning involves creating a new name for the product and some tweaking of its existing features. Like GandCrab, the Sodinokibi ransomware follows an affiliate revenue system, which allows other cybercriminals to spread it through several vectors. The attack methods include:

- Active exploitation of a vulnerability in Oracle WebLogic,
- Malicious spam or phishing campaigns with links or attachments
- Malvertising campaigns that lead to the RIG exploit kit,
- Compromised or infiltrated managed service providers (MSPs), which are third-party companies that remotely manage the IT infrastructure and/or end-user systems of other companies, to push the ransomware en-masse. This is done by accessing networks via a remote desktop protocol (RDP) and then using the MSP console to deploy the ransomware.

Sodinokibi encrypts certain files on local drives with the Salsa20 encryption algorithm, with each file renamed to include a pre-generated, pseudo-random alpha-numeric extension that's five to eight characters long. Sodinokibi looks for files that are mostly media- and programming-related with extensions such as .jpg, .png, .tif, .php, .asp,.java and more. The ransomware also deletes shadow copy backups and disables the Windows Startup Repair tool. Shadow copy and Startup Repair are technologies inherent in the Windows OS. The former is "a snapshot of a volume that duplicates all of the data that is held on that volume at one well-defined instant in time," according to Windows Dev Center. The latter is a recovery tool used to troubleshoot certain Windows problems. Deleting shadow copies prevents users from restoring from backup when they find their files are encrypted by ransomware. Disabling the Startup Repair tool prevents users from attempting to fix system errors that may have been caused by a ransomware infection.

As always, be aware of Ransomware attacks, of which Sodinokibi is one of many. We encourage you to have good backups of all data and to have a plan in place for recovery should you be infected. As always, call SIM2K for help in preparing for or mitigating any ransomware attack.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Windows 10 Finally Surges

A month after Windows users took a break from dumping Windows 7 for Windows 10, in July they made great leaps in moving away from the aging platform. According to web metrics vendor Net Applications, Windows 7's share of all personal computers plunged precipitously last month, falling 3.6% – the second-largest amount in a single month for the aged OS – to end July at 31.8%. Meanwhile, Windows 7's portion of only those PCs running Windows also plummeted, falling to 36%, a number not seen since late 2011 when the operating system was barely two years old and busily nibbling away at Windows XP. At the same time, Windows 10's share jumped by 3.1% to 48.9% of all personal computers and 55.2% of those running Windows. The monthly increase was the second-largest ever for Windows 10 (first place went to March 2019), while both percentages were records for the OS.

So, did millions suddenly drop Windows 7 and switch to Windows 10? (Net Applications' data pegged the "leaving-Windows-7" number at 61 million, compared to the "moving-to-Windows-10" number at 51 million.) There is no clear answer. The change rate wasn't implausible, as Net Applications has seen other measurements go up or down just as dramatically.

The impetus here is that the time before Windows 7 falls off the support list is very short. Windows 7's future - based, as always, on the operating system's 12-month average change - must now be more palatable to Microsoft, which earlier had to have been concerned about the operating system's stubbornness. The latest calculation says that in January 2020, when Windows 7 exits support, its user share should stand at 30.7%, a whole five points lower than the estimate after July's "no movement" measurement. That's a lot fewer PCs stranded without security updates.

Meanwhile, Windows 10 should account for approximately 62% of all Windows installations when the older OS drops off support, an increase of four points from the month-ago forecast. A year later - January 2021 - Windows 7 and Windows 10 will be at 20% and 76%, respectively.

Of special note is that the 30.7% currently forecast as Windows 7's user share at support expiration is very close to the 29% of all Windows PCs running Windows XP five years ago when it left support. For the last two years, the comparison between Windows XP's actual replacement and Windows 7's predicted performance always put the latter in the worst light; the data proclaimed that users were reluctant to give up Windows 7.

The February "out of support" mark for Windows 7 means companies should be considering a plan for moving off that platform. As we are now in Q3 of this year, budgeting for 2020 is starting, and if this is something you have not considered in initial planning, it should be. While Microsoft may be "persuaded" to keep some updates going for Windows 7, as the XP phase-out demonstrated, it is not wise to count on this. Migrating off Windows 7 needs to be planned and budgeted both from the cost of the new operating system and the manpower it will take to "touch" old devices to update. Or, this might be the time to consider new hardware as chips and storage have improved since the original Windows 7 machines were introduced. If you have older PCs around, this may well be the time to look at new. Call SIM2K to let us help you with a strategy for your company as Windows 7 moves out of support in 2020.

"Random Tid-Bytes"

Capital One Data Breach

A data breach to Capital One servers in March exposed the personal information of nearly 106 million of the bank's customers and applicants. The hack, which included US and Canadian customers of the banking and credit card company, comes a week after the settlement reached between Equifax and the Federal Trade Commission concerning a hack in 2017 that affected 147 million customers. According to Capital One, the breach on March 22 and 23, 2019, resulted in the hacker gaining access to personal information related to credit card applications from 2005 to early 2019 for consumers, applicants and small businesses. Capital One detected the breach on July 19. Among the personal data exposed were names, addresses, dates of birth, credit scores, transaction data, Social Security numbers and linked bank account numbers. About 140,000 Social Security numbers and 80,000 linked bank account numbers were exposed, Capital One said. And for Canadian credit card customers and applicants, approximately 1 million Social Insurance Numbers. Capital One said, however, that no credit card account numbers or login credentials were revealed in the hack. Capital One said it will contact by letter U.S. individuals whose Social Security numbers or linked bank account numbers were part of the hack. Affected individuals can probably expect to hear the week of August 5. At the moment, Capital One doesn't have a website that lets you check for yourself, unlike with the tool Equifax released to see if you were part of its data breach. Capital One said it has fixed the exploit the hacker used to access the data and has worked with federal law enforcement on the breach. The banking company said it will reach out to customers who were part of the hack and will offer free credit monitoring and identity protection to those customers affected by the breach.

Apple Acquires Intel Smartphone Chip Business

Apple's decision to invest a billion dollars in purchasing most of Intel's modem development unit will speed up development of their 5G smartphone product, experts believe. Apple takes control of over 17,000 wireless technology patents as a result of the deal. These include patents that relate to cellular standards, modem architecture, modem operation, and chip engineering. This gives Apple a much stronger voice in conversations around future mobile standards. This is important, as 5G and 5G services are expected to unlock the next chapter in digital transformation. Apple needs to ensure it's a peer player in that space. Apple is only acquiring Intel's smartphone modem business. Intel will still be permitted to develop modems for non-smartphone applications, such as PCs, internet-of-things (IoT) devices and autonomous vehicles. This also relates to 5G-related network infrastructure. Apple settled the lawsuit with Qualcomm earlier this year, meaning it is likely the 2020 5G iPhones will carry modems from Qualcomm. The acquisition is expected to help Apple develop its own 5G modems for use in its devices and not be yoked with an outside vendor like Qualcomm moving forward.

Chrome On the March

Chrome again jumped in user share. According to Net Applications, Chrome's July user share climbed by 2.3% to end the month at 68.6%, a record for Google's browser. The month's increase was the largest since August 2016. In five of the past seven months, Chrome has held more than two-thirds of global browser share, a statement to its grip on the market. Firefox shed user share again in July, dropping to 8.3%, and Edge slipped to 5.8%.

The Dark Side of Cloud Computing

Long ago, a server was something that was yours and yours alone. You would set the specs, collect bids, fill out a purchase order, and then take delivery on the machine so it could be carefully installed and tested in the server room just down the hall from your desk. You could walk over, touch it, check that the LED was burning bright, and feel secure listening to the quiet hum of the fan.

Now you might not have anything to do with your hardware. Some people click on a webpage of a cloud company to create an "instance" and spend a few moments configuring the build routine, but after that the work is left to some robot deployment routines. The disconnection with our hardware is growing even deeper as the "serverless" buzzword grows more common. Of course, the companies don't literally mean there's no server in the loop. They just mean that you shouldn't be concerned about those boxes of chips whirring away somewhere else. Just give us your few lines of code and we'll make sure that some piece of silicon in our back warehouse will run it.

Many of these mysteries are labor-saving and stress-saving innovations. Being left in the dark means not wasting our time thinking about any of the details about memory configuration or drive partitioning or whether that broken DVD-ROM tray matters. But sometimes a bit too much is being swept under the rug. Sometimes a bit too many details are removed from the discussion before we click that button and agree to the terms of that seemingly endless contract that no one ever reads. We're not saying that you should be staying up late worrying about these things. But here are questions we often face when dealing with Cloud Computing.

Where is the server?

It's in the cloud. That may be all we know. The companies may say our instance is running in New York or Karachi but that's all we get. Often the best we can do is know the name of the city or maybe just the country. Should we care about the actual address? Maybe masking the location of the building itself is a security feature – if we don't know the physical location of the box, well, the bad guys will be just as confused. But, sometimes we need to know the physical location of the data center when it comes to issues like tax laws or legal issues with jurisdiction, export laws or letting data cross a border, or the general security of the neighborhood where your data "lives."

What is the CPU?

Chances are you won't know the manufacturer or the model number or any detail whatsoever about the "box" where your data will run. The cloud companies sell you instances with cryptic names like "m1" or "large," but that doesn't mean much. The "m1" and the "m2" may not have anything to do with each other. They're just names. Some cloud companies try to measure the "virtual" CPU power you're buying and then let you dial up just the right amount. Again though, sometimes the hardware makes a difference. Sometimes there are security holes or glitches that can be traced to particular chips, or some chips run certain algorithms better than others.

What kind of memory?

For a long time we thought about whether it was worth it to install faster memory or if some RAM was better or more stable than others and had opinions about brand names and technological approaches. Now we don't know just how good the hardware might be. This is one thing the cloud company engineers are supposed to worry about so we don't have to. Maybe our programs are crashing because of bad RAM. Maybe it's because of our own terrible code. We'll never know.

What kind of drives?

Some cloud companies brag about using SSDs. Some brag about using faster hard disks. Some just rent us 25 gigabytes of storage and not get into the details. But not all disk drives have the same reliability ratings. Not all flash memory is created equal. Did things fail because of some bad sector on the hard drive or was it something in the code? Cloud companies may employ a mix of drives so you can't be sure from server to server even staying with one company.

Other chips are even more mysterious

Most people spend even less time thinking about the rest of the computer. We talk about the CPU and sometimes the GPU, but does anyone outside the networking team discuss the NPU, the Networking Processing Unit? They have firmware of their own and the clouds have elaborate, reconfigurable networking layers with some of the most sophisticated semantics around. While we're fussing over obvious points of weakness, has anyone spent much time thinking about what a hacker can do with a network card?

What kind of technology?

Sometimes we don't even know the right buzzword to use to describe a service. Amazon's Glacier storage is one of the cheaper places for Cloud computing, but Amazon won't explain what technology they're using. Is it built from racks and racks of slow magnetic hard disks? Or perhaps they burn the data onto stacks and stacks of Blu-ray disks? Or maybe they use magnetic tape loaded by robot arms? Maybe they've used two or three different technologies so they could switch the cost curves around? It's all a mystery. All we know is how much it costs per gigabyte and how slowly it might take to retrieve the information.

What's going on?

Sometimes we'll never find out what's going on at all. Moving to the cloud doesn't remove the dangers of bad events like power outages, imploding disk drives, or ransomware, but it does cut us off from learning what's going on. In your server rooms, everyone is right in front of you. You can get to the bottom of the issue. In the cloud, you probably won't know anyone who is handling the problem. At best, you communicate through e-mails and trouble tickets. Even then, the lawyers, the managers, and the PR flacks get in the way and the only thing we get is carefully worded CYA. At best, we'll learn "mistakes were made." At worst, we'll hear nothing.

For something that is supposed to be "time saving and easy" Cloud computing brings a new raft of problems. We can help you assess any Cloud provider if you must move that way.

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com