SIM2K
Adapting Technology to Your Business Needs

11 • 20
Information
you can use

SIMformation

Trump Twitter Hack Shows Need for 2FA

Donald Trump's Twitter account was allegedly hacked ater a Dutch research says he correctly guessed the President's password, "maga2020!", Dutch media reported. Victor Gevers, a security expert, had access to Trump's direct messages, could post tweets in his name and change his profile, according to newspaper reports.

Gevers – who previously managed to log into Trump's account in 2016 – apparently gained access by guessing Trump's password. He tried "maga2020!" on his fifth attempt and it worked. Maga stands for Trump's oft used campaign slogan Make America Great Again.

"I expected to be blocked after four failed attempts. Or at least would be asked to provide additional information," Gevers told reporters. Twitter, however, denied the report. "We've seen no evidence to corroborate this claim, including from the article published in the Netherlands today. We proactively implemented account security measures for a designated group of high-profile, election-related Twitter accounts in the United States, including federal branches of government," a Twitter spokesperson said in a statement.

However, Gevers told De Volkskrant the ease with which he accessed Trump's account suggested the president was not using basic security measures like two-step verification. Allegedly gaining access to Trump's Twitter meant Gevers would be able to connect with 87 million users – the number of Trump's followers – and sent him into a bit of a panic.

"So, he tries to warn others. Trump's campaign team, his family. He sends messages via Twitter asking if someone will call Trump's attention to the fact that his Twitter account is not safe. He tags the CIA, the White House, the FBI, Twitter themselves. No response," the paper reported. A day later, Gevers noticed that two-step authentication had been activated on Trump's account. Two days later, the Secret Service got in touch. According to De Volkskrant, they thanked him for bringing the security problem to their attention.

Remarkably, it wasn't the first time Gevers has gained access to the president's Twitter account. In 2016 he and two others guessed Trump's password and got into the account. Back then Trump's password was "yourefired", his catchphrase from the NBC TV reality show, "The Apprentice."

Two-factor authentication (2FA) – also known as two-step verification or multifactor authentication – is widely used to add a layer of security to your online accounts. The most common form of two-factor authentication when logging into an account is the process of entering your password and then receiving a code via text on your phone that you then need to enter. The second layer in two-factor authentication means a hacker would need to steal your password along with your phone in order to access your account.

After you enter your password – the first authentication factor – the second factor usually arrives by SMS. That is, you get a text with a numerical code that you'll then need to enter to log into your account. Unlike a PIN code for a debit card, a 2FA code is used only one time; each time you log into that account, you'll be sent a new code. Many sites and services, including Amazon, Dropbox, Google and Microsoft, give you the option of using SMS or an authentication app. Twitter is the biggest example of a site that forces you to use SMS.

The alternative 2FA process is to use an authentication app like Duo, which SIM2K recommends. Receiving codes via SMS is less secure than using an authentication app. A hacker could intercept a text message or hijack your phone number by convincing your carrier to transfer it to another device.

Duo's 2FA solution only requires users to carry one device – their smartphone, with the Duo Mobile app installed on it. Duo Mobile is available for both iPhones and Android, as well as wearables like the Apple Watch.

With support for a large array of authentication methods, logging in via push notification is fast and easy with Duo Mobile. SIM2K recommends using Duo Push as your second factor, because it is the most secure and can protect against man-in-the-middle (MITM) attacks, but with Duo's flexibility and customizability, we can work with you to find the authentication method that meets the unique needs of your on-line experience.

Other types of two factor authentication are susceptible to phishing attacks, but Duo's push-based 2FA combats that vulnerability by replacing access codes with push notifications. When you attempt to access information, a push notification is sent to your phone. The notification includes information about the login attempt, such as location, time, IP address, and more. Then you simply confirm that the information is correct and use your phone to accept the authentication request.

For more information on two-factor authentication, and the security options offered by Duo, please contact SIM2K.

Microsoft – What's the Deal?!

Users are accustomed to having Windows updates being a gamble, but Outlook? Office!? What's going on here? Every few months Microsoft issues another disastrous Windows update or patch, but seemed to be OK with their Office 365 Software-as-a-Service offerings. So much for that idea.

Starting in June, Microsoft's services plunged downhill. First, Outlook just stopped working for many people. Then in July, all Outlook clients and services came to a halt. As some tech bloggers said, "Come on, Microsoft. This is e-mail 101. How hard can it be? How can you keep blundering like this?"

But as it turned out, things got far worse. As we noted in SIMformtion last month, Office 365 and Outlook users got a September surprise when starting on Sept. 28 and lasting through the next day, Microsoft users around the world found they couldn't sign into Microsoft and other programs that use Azure Active Directory (Azure AD) for authentication. Microsoft quickly figured out what was wrong – a beta service update made it into Azure AD backend services, and everything went haywire. So, the company "fixed" it using an automated rollback…, which failed. Six hours later, the services were finally up again.

But on Oct. 7, Microsoft's Office 365 and Outlook crashed for an entire day. Microsoft said this time that if customers were using resources that operated between regions on Azure network infrastructure they would run into these problems. How do you know, when using Office 365, whether you're working on, say, a document residing in a US East availability zone, while your application's running in on Pacific time? Short answer: You don't.

This time the problem was a "deliberate change (that) was applied to [Wide Area Networking] WAN resources causing connectivity latency or failures between regions." To fix it, the Azure team rolled things back to a healthy configuration. This time it worked.

The common theme here is that Microsoft isn't doing enough work to make sure its fixes and upgrades don't break systems. Quality assurance needs to be job one. After all, if your users can't count on getting their work done, they will move to options like Google Workplace. This has always been the weak point of the Microsoft business model, as jokes about "bugs and viruses" have abounded for years for Windows. But the Cloud service software was sold on the "tested and proven, factory-maintained" claims, which once again have come up short. So keep this in mind when considering what mix of software you want for your company and the viability of these services in the 24-hour business cycle.

QR Code Scams

Just when we thought the QR code was on its way out, the pandemic has led to a return of the scannable shortcut. COVID-19 has meant finding a digital equivalent to things normally handed out physically, like menus, tour guides, and other paperwork, and many organizations have adopted the QR code to help with this. And so, it would seem, have criminals. Scammers have dusted off their book of tricks that abuse QR codes, and we're starting to see a resurgence in scams.

A Quick Response (QR) code is nothing more than a two-dimensional barcode. This type of code was designed to be read by robots that keep track of items in a factory. As a QR code takes up a lot less space than a legacy barcode, its usage soon spread. Smartphones can easily read QR codes – all it takes is a camera and a small piece of software. QR codes gained some popularity among advertisers because it was easier for consumers to scan a code than to type a long URL. But people couldn't tell from a QR code where scanning would lead them, so they got cautious and QR codes started to disappear. Then along came the pandemic and entrepreneurs had to get creative about protecting their customers against a real life virus infection.

For example, given the fear of spreading COVID-19 through many people touching the same menu in a restaurant, businesses placed QR codes on their tables so customers could scan the code and open the menu in the browser on their phone. Clean and easy, right? Unless a previous visitor with bad intentions had replaced the QR code with his own. Enter QR code scams. Like clickjacking, where someone gets paid by luring others to clicking on a certain link. Rather than see the restaurant menu, instead, the replaced QR code takes them to a sleazy site and the clickjacking operator gets paid his fee.

Another trick is the small advance payment scam. For some services, it's accepted as normal to make an advance payment before you can use that service. For example, to rent a shared bike, you are asked to make a small payment to open the lock on the bike. The QR code to identify the bike and start the payment procedure is printed on the bike. But the legitimate QR codes can be replaced by criminals that are happy to receive these small payments into their own account.

Phishing links can just as easily be disguised as QR codes. So, for example, if someone is expecting to login to start a payment procedure or to get access to a certain service, the scammers may place a QR code there.

So treat QR codes with caution. Do not scan a QR code embedded in an e-mail. Treat them the same as links because, well, that's what they are. Check to see whether a different QR code sticker was pasted over the original and, if so, stay away from it. Or better yet, ask if it's OK to remove it. And, use a QR scanner that checks or displays the URL before it follows the link. It is unfortunate that the "bad guys" take advantage of a pandemic, but so it goes, so be alert when you see QR codes.

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.

Still Working from Home?

Working from home is hardly new, but the COVID-19 pandemic has made it an unplanned requirement for many office and knowledge workers. Even when the crisis eventually recedes, many employers have discovered that they don't need large office buildings, and many employees will have discovered that they don't need to be in the office every day or spend hours commuting.

But many people have set up makeshift home offices for the pandemic that won't work well for the long term. In addition to having the right equipment, the physical setup is critical, especially around avoiding repetitive strain injuries that a bad setup can cause.

A long-term home office should ideally be a separate space in your home that is properly outfitted for work. Do as much of the following as you can to create an effective, safe workspace for the long term. Ideally, you would use a small room that can hold a desk and computer equipment and whose door can be shut for the essential need to separate work life from home life. Most people don't have spare space, but many people can convert a guest room into a dual-purpose space: an office most of the time and a guest room when people visit.

Your space needs a desk or table that is at work height. The industry standard is 29" from the floor to the top of the work surface. Many desks and tables have adjustable height, usually through their feet. But that industry standard is based on writing on paper, not using a keyboard and mouse. That's why keyboard trays pull out from below the work surface and are typically an inch or two lower than the desk or table height. If you have space for a keyboard-and-mouse tray (it must be wide enough for both!), get one. You know your work surface is at the correct height if, when you sit up straight, your forearms are parallel to the ground and your wrist is not bent up or down when you type or mouse. The top surface of your wrist should essentially be on the same plane as the top of your forearm, with your fingers dangling slightly down to the keyboard. Bending the wrists for prolonged periods is an easy way to cause injury.

Get a large monitor (maybe two) for your home office. Your monitor should line up so that if you look straight ahead when sitting straight, your eyes are at a height of 25% to 30% below the top of the screen. That way, you keep your shoulders level and don't hunch your back. There are a lot of bad chairs out there that can injure you over prolonged computer use. Dining chairs and deck chairs, for example, rarely are at the right height, and they don't always encourage the needed upright posture.

The bandwidth within your home matters too. The best connections are wired Ethernet ones, so if possible, connect your computer to your router via an Ethernet cable; that's especially important if you do video or other bandwidth-intensive work. Wi-Fi is fine for basic office work, so if you can't wire your computer to your router, use Wi-Fi.

"Random Tid-Bytes"

USB-C Connectors

You've probably noticed something strange about many of the latest phones, tablets and laptops at your company: The familiar rectangular Type-A USB ports are gone, replaced by smaller oblong connectors. USB-C has taken over at work, at home and at school. USB-C is now part and parcel of most laptops, phones and tablets made today. Even the latest MacBooks and Chromebooks are part of the movement to USB-C. Because the USB-C plug is symmetrical, it can be inserted either way, eliminating the frustrations of earlier USB ports and putting it on a par with Apple's reversible Lightning plug. Most USB-C ports are built on the second-generation USB 3.1 data-transfer standard, which can theoretically deliver data at speeds of up to 10Gbps – twice as fast as USB 3.0 and first-gen USB 3.1, which both top out at 5Gbps. The key is to get devices that say "USB 3.1 Rev 2," "USB 3.1 Gen 2," "SuperSpeed USB 10Gbps," or "SuperSpeed+" to get support for the faster spec. To make sure the data gets through at higher speeds, always get high-quality cables. They will often have the SuperSpeed logo and a "10" on them to show they're capable of moving 10Gbps.

Ransomware Payments Nixed by Treasury Dept.

In October, the US Treasury Department's Office of Foreign Assets Control (OFAC) warned organizations making ransomware payments that they risk violating economic sanctions imposed by the government against cybercriminal groups or state-sponsored hackers. The advisory has the potential to disrupt the ransomware monetization model, but also puts victims, their insurers and incident response providers in a tough situation where this type of attack could cost much more and take much longer to recover from. "OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to US jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC," the Treasury Department said. The value of ransom demands has also skyrocketed, varying between hundreds and millions of dollars per victim. Attackers keep pushing the limits of what they can ask and that's partly because cyberinsurance policies often cover the costs of ransomware attacks. Little information is available on how many private companies choose to pay ransoms, because there are no regulatory obligations to report such incidents, but indirect evidence suggests that paying ransomware is common. Examples of groups or individuals that have ties with ransomware attacks and are on the Treasury Department's sanctions list include Iran, linked to the SamSam ransomware; North Korea's state-sponsored Lazarus group, which is linked to the WannaCry attack; and a Russian cybercriminal organization which is behind the Dridex botnet. The threat to US businesses of being extorted – as well as of running afoul of OFAC – reinforces the importance of cyber best practices. SIM2K can help you with securing data and ensuring backups are in place, as well as training staff on how to identify potential ransomware ploys.

Got Macs? But Using Microsoft?

Microsoft has released updates to several iOS-based Office programs. Teams gains Caller ID and spelling tools and added file-sharing improvements, Yammer gains an iOS widget, and Microsoft Remote Desktop fixes to better link to a Windows device. So if you are a home worker using iPads or Macs, you can better replicate the environment found on your office Windows PC.

Google Faces Anti-Trust Action

The US Department of Justice has filed a landmark lawsuit against Google, accusiong the company of illegally holdingmonopolies in search and search advertising/ This is the culmination of a year-long plus look into alleged anti-competitive practices at the company. This is a significant event in that it is the first such antitrust case in the IT industry in decades (the Microsoft lawsuits of the 1990's).

The government alleges that Google has violated antitrust laws to act as a "gatekeeper" to the Internet. The documentation says the company has unlawfully blocked out competitors by reaching deals with phone makers including Apple and Samsung to be the pre-set default search engine on their devices. The complaint also says Google has abused the dominance of its Android operating system to force manufacturers to pre-load Google apps onto phones.

"As the antitrust complaint filed today explains, [Google] has maintained its monopoly power through exclusionary practices that are harmful to competition," Jeff Rosen, US deputy attorney general, said. "If the government does not enforce the antitrust laws to enable competition, we could lose the next wave of innovation. If that happens, Americans may never get to see the next Google."

Eleven states, all with Republican attorneys general, are joining the lawsuit as plaintiffs: Arkansas, Florida, Georgia, Indiana, Kentucky, Louisiana, Mississippi, Missouri, Montana, South Carolina and Texas. The lawsuit marks the latest in a series of moves by the US government to put big tech under a more intense microscope.

Google's power stems from its massive digital ad business that brings in about 85% of the company's roughly $160 billion in annual sales. That operation is led by the namesake search engine, which processes around 90% of searches done online around the world and is considered some of the most prime positioning on the Internet.

The tech giant denied the allegations of anti-competitive behavior. "[Today's] lawsuit by the Department of Justice is deeply flawed," said a Google senior vice president. "People use Google because they choose to, not because they're forced to, or because they can't find alternatives."

Google's antitrust legal woes may be just beginning. Separate from the DOJ announcement, seven states including New York and Colorado said they are concluding their own investigations in coming weeks, and if warranted will consolidate their findings with the Justice Department case.

The DOJ lawsuit comes as tech giants face a reckoning over their size and influence. Legislators and regulators are concerned over how that power might ultimately harm consumers, especially by choking off competition from smaller players in Silicon Valley. Apple Amazon and Facebook are also under investigation. by the House Judiciary Committee. A subcommittee issued a 449 page report earlier in October accusing these companies of "abuses of monopoly power." The Judiciary's scrutiny of Gogle focused on the company's alleged promotion of its own products over those of rivals. "Evidence shos that once Google built out its vertical offerings, it introduced various changes that had the effect of privileging Google's own inferior services while demoting competitors' offernings," the report states.

Google has faced scrutiny from federal regulators in the past. In 2013, the Federal Trade Commission wrapped up a two-year investigation into Google after allegations of biased search results. The agency, however, decided unanimously that Google wasn't violating antitrust laws.

However, this new lawsuit heavily criticizes Google's business contracts with outside partners. The complaint says the tech giant "locks up" search distribution on Android, which powers almost nine out of every 10 smartphones shipped globally. The lucrative contracts have even resulted in Google and Apple, two bitter rivals, to work together. Google's biggest smartphone deal is with Apple, paying the iPhone maker $8 billion to $12 billion in ad revenue a year to make Google search the default on Apple devices. The deal extremely is beneficial to both companies: The lawsuit says the agreement accounts for 15% to 20% of Apple's annual profits. The suit also says almost half of Google's search traffic last year came from Apple devices. The deal is so important that Google views losing it as a "Code Red" scenario, according to the DOJ's complaint.

In a lengthy blog post, Google denied any wrongdoing when it comes to the search deals it makes with other companies. Google, which spends billions of dollars a year on those deals, compared the practice to a cereal brand paying for "eye level" placement on a grocery store shelf, instead of having the product stocked on a lower shelf.

Many in the IT industry believe that this attempt to reset the technology balance of power against Google will likely come to nothing. At most, they expect to see Google pay a small – for Google – fine and re-draft its advertising contracts. However, this is the first salvo in recent years directed against dominant technology companies, and may or may not be the first of many more suits to follow against social media and other market-leading tech companies.

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