SIM2K
Adapting Technology to Your Business Needs

11•18
Information you can use

SIMformation

Do You Even Bother to Answer Anymore?

Users have found themselves at war with a constantly burgeoning trend of unwanted calls that plagues smartphones, traditional landlines, and VoIP devices. And while there are tools to help consumers address robocalls, scam calls, and spoofed calls, contrary to popular opinion, US telecommunications companies have the technology to protect customers themselves—they just haven't done it yet.

To this day, some of these companies are still hemming and hawing about aggressively block robocalls, putting technology on the back burner. Another roadblock to the adoption of new blocking technologies is the existence of legacy phone systems that may not be up to the task. As a result, addressing the robocall problem is left mostly in the hands of consumers.

But the spam problem isn't going to go away on its own. According to a report from First Orion, a company that provides call blocking, by 2019 almost half of cellphone calls in the US will be scams. We're also seeing a new and emerging trend of non-English speaking robocallers targeting immigrant communities. Thankfully, lawmakers have taken note of the rising tide of phone spam and decided to do something about it.

Regulators and lawmakers have long recognized that consumers cannot solve this seemingly impossible problem. After all, they are just as affected by the deluge of unwanted calls as the average Joe, and have similarly witnessed the consistent surge of phone spam over the last few years. Thus, several new legislation and rules have been passed and/or introduced to help address robocalls and other illegal calls. They include:

DNO list

In the fourth quarter of 2017, the FCC approved rules that authorize voice service providers—mobile phone carriers, landline carriers, and VoIP carriers—to instantly block telephone numbers in a "Do-Not-Originate" (DNO) list. A DNO is a set of phone numbers that do not or cannot make outgoing calls. The nature of calls received from numbers that belong in the DNO are always fraudulent, and instantly blocking them can curb unwanted calls. While those in the telecommunications profession agreed that a DNO list would help, they also believed that scammers would eventually find a way around it.

RAY BAUM'S Act

Officially designated as H.R. 4986, the Repack Airwaves Yielding Better Access for Users of Modern Services, or RAY BAUM'S Act, gives power to the Federal Communications Commission (FCC) to strengthen the US's critical telecommunications services and increase the deployment of 5G. RAY BAUM'S Act, which was passed in March 2018, is also meant to "advance proposals that would help the FCC and law enforcement protect consumers from fraudulent telephone calls, and to educate Americans about their options to stop these illegal calls."

Florida Call-Blocking Act

Bill number CS/HB 1267, or the Florida Call-Blocking Act, gives power to telecommunications service providers to block calls from bogus numbers, spoofed numbers, and numbers that impersonate local numbers. It also authorizes telecoms to stop blocking certain calls, such as emergency calls.

ROBOCOP Act

The Repeated Objectionable Bothering Of Consumers On Phones, or ROBOCOP Act, if passed, will give more power to telecom customers to pick and choose the type of calls they want to receive and block. It will also give users the right to take legal action against telecoms that violate this act. Telecoms will also be required to verify the accuracy of caller IDs and offer free, optional robocall-blocking technology to their customers.

Additional technologies and strategies have surfaced that some consumers use and swear by their success in blocking unwanted calls. The list below has some steps you might consider:

- Consider using a Google Voice number to screen and forward calls. Google Voice has been around for almost a decade, and users have found that using Google's free phone number as their primary number instead of their real number has helped filter out unwanted calls.
- Use your phone's "Do Not Disturb" feature. Doing so, in effect, will whitelist calls from your contacts and block everything else. You can do this on iOS by opening the Settings app, flipping on Do Not Disturb—don't give it a schedule—and then tap "Allow Calls From" and pick "All Contacts." On Android, you can do this by going to Settings > Sound > Do Not Disturb.
- Think about purchasing a phone spam-blocking security app for your smartphone, such as Malwarebytes for iOS or Malwarebytes for Android, both of which will block spammy or malicious text messages as well.

More unwanted call tactics will spring up in the future, no doubt – experience has taught us to expect it. Thankfully, there is movement from regulators, law enforcement, and several telecoms and private companies to address the problem of unwanted calls. It's great to know we're not entirely defenseless in this fight against phone spam. So, let's make use of the tools available to us, take advantage of protection services offered by your phone provider, and continue to hold telecom companies accountable for preemptively blocking unwanted calls.

Is Your Desk Spying On You?

On the last day of National Cyber Security Awareness Month, which was also Halloween, The National Security Agency (NSA) released something "scary" – if you value privacy and security. The NSA has warned that "smart" office furniture may be spying on your activities!

Why is the NSA talking about IoT office furniture? Because the agency has to buy desks and chairs the same as any other business. If that furniture is "smart" then, that's one more potential entry point into a network or an avenue for threat actors to gather sensitive information.

Apparently, connected office furniture is part of a growing business trend; IoT connectivity allows for the wireless tracking of how efficiently the workforce uses equipment and spaces. Data from integrated sensors in "smart" furniture is supposed to help companies improve workers' productivity and potentially maximize existing spaces such as use it or lose it.

An October 2018 research report on China's Internet of Things delved into how China is becoming more dominant in the IoT arena and is therefore in a position to dictate rules of international standards, including those that impact the security of IoT devices against unauthorized access. The report looks at previous and known vulnerabilities in Chinese IoT products and discusses how Beijing's "research into IoT security flaws and its growing civil-military cooperation raise concerns against gaining unauthorized access to IoT devices and sensitive data."

While we mostly hear about back-door flaws that enable unauthorized access to IoT devices, the report points out that "even authorized access to these devices may reveal large amounts of sensitive data on U.S. citizens." That "authorized access to IoT data of U.S. consumers will only grow as Chinese IoT companies leverage their advantages in production and cost to gain market share in the United States."

You may not think that "smart" furniture will become an actual big thing, but some said that about other items – and good luck trying to find a decent vehicle or even a TV that isn't connected. So if you want "dumb" furniture, then maybe you should consider shopping for it sooner rather than later when more office furniture will come with IoT connectivity.

Bugs Plague Windows 10 Update

Microsoft has had serious issues with the Windows 10 "October 2018 Update," forcing the company to withdraw this update from distribution in early October.

Although Microsoft officially released the refresh on Oct. 2, four days later it barred access to the upgrade via Windows Update, told those who had installed it to stay off their PCs and warned users who had downloaded but not installed it to trash the disk image. The reason? Some users reported that the upgrade deleted all files in several folders, including the important Documents and Photos directories.

Mid-month, the Windows servicing group told customers that the bugs had been fixed, but rather than put the update out for general use, released it only to volunteer "testers" who are part of the Windows Insider preview program. With the release of Windows 10 1809 now postponed by at least four weeks, the delay has impacted the upgrade's support timeline.

According to the company's "Windows Lifecycle Factsheet" support for this update will expire in April, 2020 for Home and Pro versions and April 2021 for Enterprise and Education versions. If Microsoft does not restart distribution of Windows 10 October 2018 Update soon, it would shortchange customers on support. Rather than the promised 18 months for Windows 10 Home and Windows 10 Pro, it would instead provide support for 17 months and Windows 10 Enterprise and Education would get less than the pledged 30 months.

"If Windows-as-a-Service is in fact a hosted service, if general availability is paused, is the support window of 18 or 30 months extended by the number of days for each pause?" asked IT insiders in tweets aimed at the company. But, it remains unclear if Microsoft will address the support shortfall, and if so, how.

Microsoft could extend support for the October update in the same way it did for the delayed April update, extending support for the full 18 months (Home and Pro versions) or 30 months (Enterprise or Education versions). For example, if the firm re-started distribution on Friday, Nov. 2, it could restate end-of-support for Home and Pro as May 12, 2020, giving users 18 months and 10 days of security patches and bug fixes. However, when asked whether Microsoft will add more time to 1809's support, a spokeswoman for the company declined to comment.

The other question is why Microsoft again allowed a "buggy" release to hit the streets, especially if it was as damaging as depicted. Deleting the Documents folder, which by default is where Windows wants to save all your work, it a major problem. This again points out why it is best to not be at the forefront of installing updates from Microsoft. SIM2K customers on our Critical Updates program have the benefit of our automatic "delay" in applying these as we do wait to see if there are any bugs or other fall-out from these updates before we apply them to your PCs. Contact us for more information on Critical Updates.

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.

Password Security

In the past year, security teams have seen both large and small organizations hit by high-profile breaches. They've also witnessed the cost, not just monetary, but in loss of reputation for both the affected organizations and security leaders. Layered on top of that are new privacy and security regulations that redefine many aspects of how security organizations do their jobs.

These trends and events are driving companies to take IT security more seriously. The 2018 U.S. State of Cybercrime survey is conducted annually by CSO in partnership with the US Secret Service and CERT. Here are some of the findings from this study.

One notable change from last year's survey is in the average IT security budget. It increased to $15 million, up from $11 million. That's nearly a 27% rise, and it is another indicator that security is top-of-mind among business leaders. Fifteen % of respondents said their IT security budget was more than $10 million. Interestingly, 37% said their IT security budget was less than $250,000. That suggests that some companies represented in the survey spend significantly more than $10 million given the average spend of $15 million.

The average number of security events at respondents' companies continues to decline – down to 107 from 148 in 2017. The disparity between enterprise-level organizations and SMBs is large, however. Enterprises reported 196 events, while SMBs reported only 24. Those numbers might seem low depending on how you define a security event, as the survey was a bit vague as to defining an "event." A better indicator of the seriousness of security events is whether an organization had to notify individuals or regulators. Twenty-four % of enterprise respondents and 12% of SMB respondents said they had to notify individuals impacted by a breach. Twenty-three percent of enterprise respondents and 5% of SMB respondents had to notify regulators of a breach.

While the vast majority (79%) of respondents feel they have the expertise to address risks, most organizations leave their employees and management under-trained on security. Only 15% of respondents said their organizations do continual security training. More companies (29%) only provide training once a year. Most respondents felt that the group in their organization that needed the most training was the c-suite (55%) followed by low-level staff (43%) and, interestingly, the IT department (34%). Since more than half (53%) of organizations represented in the survey were victims of a phishing attack, much of the training done in 2018 was focused on preventing it. Thirty-nine % commonly use phishing and social engineering behavior testing.

SIM2K offers training and testing of your security program, including mock phishing attacks, so please call us to discuss how we can help bolster your security profile.

"Random Tid-Bytes"

Microsoft Invokes Price Increase for Retail Office

Microsoft has increased prices for the retail versions of Office 2019 by 10%, similar to the price hikes announced in July for commercial volume licenses. Then, Microsoft said Office 2016 would bump up 10% and other licenses such as Windows Server and Exchange Server would increase as much as 30%. These increases are for the perpetual licenses, the one-time payment system most people know– buy it and use it forever – rather than the subscription model that Microsoft is moving towards with a monthly fee being charged (Office 365). This price hike means that Office 2019 Professional will now retail for $439.99 for one licenses version. These price hikes are part of the company's strategy to push users to the subscription model, which Microsoft confirmed, saying that this will "highlight the benefits of our pricing for a cloud-first world" meaning that the real price breaks will now be offered for those opting for the subscription software.

Facebook Hack

Facebook announced that its social network had been hacked, resulting in 30 million accounts that were directly impacted. Attackers exploited a feature in Facebook called "View As," which essentially shows how your profile looks to others. The flaw enabled them to get hold of so-called Access Tokens, which allowed them to be logged in as genuine Facebook users without having to use their password. The feature has, for now, been turned off and the underlying vulnerability fixed. A law enforcement investigation is ongoing to determine the full scope of this hack and identify the perpetrators. Facebook says they have taken actions and that there is no need for users to reset their passwords, although it is a good opportunity remind users that passwords should be complex and not reused across multiple services.

Wi-Fi 6 Coming in 2019

Wi-Fi 6 – aka 802.11ax – will begin to make its way into new installations in 2019, bringing with it a host of technological upgrades aimed at simplifying wireless-network problems.
It is designed to operate in today's increasingly congested radio environments. It supports multi-user, multiple-input, multiple-output (MU-MIMO) technology, meaning that a given access point can handle traffic from up to eight users at the same time and at the same speed. Previous-generation APs still divide their attention and bandwidth among simultaneous users. Better still is orthogonal frequency division multiple access (OFDMA), a technology borrowed from the licensed, carrier-driven half of the wireless world. What this does is subdivide each of the available independent channels available on a given AP by a further factor of four, meaning even less slowdown for APs servicing up to a couple dozen clients at the same time. The process of introducing a new Wi-Fi standard to the market can be lengthy, as chipsets follow draft standards by a few months, consumer APs for the early adopter follow a few months later, enterprise a few months after that, and finally wide availability of compatible endpoints after a year or more. Therefore, businesses should start planning for Wi-Fi 6 in 2019, but active use of the standard in production might not take off for another year. We will keep watch on the progress of this new standard and when Wi-Fi 6 is generally available and working as designed.

Anti-Virus – Still Plays a Role

Traditional signature-based anti-virus is notoriously bad at stopping newer threats such as zero-day exploits and ransomware, but it still has a role as part of a multi-layer endpoint security protection strategy. The best anti-virus products act as the first layer of defense, stopping the vast majority of malware attacks and leaving the broader endpoint protection software with a smaller workload.

Antivirus products create a signature for each piece of malware that is detected in the wild, but it requires someone to be infected to get the process started. And, it could be days or months until the "fix" reaches everyone in the user universe, giving time for this attack to spread through the enterprise causing damage or stealing personal information.

In fact, at a recent security conference, 73% of attendees believe that traditional anti-virus is obsolete. There is data to support this belief, as a test was conducted that calculated how well leading traditional anti-virus products did at spotting zero-day threats. Traditional anti-virus missed 38% of malware attacks caught by next-generation tools, an 8% increase in the failure rate in one year.

This is due, in part, because the "bad guys" are getting smarter. Not only are they better at quickly generating new versions of existing malware, tweaked just enough to evade detection, but also developing new malware that can't be picked up by traditional anti-virus software. When security experts look at what companies are doing for protection, only 50% of those surveyed have installed next-generation tools, and of those, only 37% are actually using them. Companies recognize this threat, as 70% rate this as their #1 concern, but only 29% say that traditional anti-virus provides the protection they need.

But, security experts say that the traditional AV tools still have a role to play. The next-generation tools take time and use up network bandwidth and CPU resources. The "old" AV products are fast, cheap and don't require lots of resources to work. And, as mentioned earlier, they still provide that first line of defense to weed out the bulk of malware attacks that happen on a daily basis.

This then lets the next-generation tools tackle the more complex threats that get past the traditional AV screen. The threat can be analyzed or quarantined and dealt with by the more sophisticated tool in a more focused fashion rather than dealing with all threats. Many of these new tools involve behavior analytics and machine learning, requiring more processor power. Or they run behavioral tests before permitting user access, impacting productivity as the user waits for the suspect data to be released. And, when a new threat is detected, additional work is required to mitigate the threat and generate a defense against re-infections in the future. Running traditional signature-based anti-virus screens saves human effort and reduces false positives and time delays.

Recognizing the role of traditional AV, security companies are now combining the old and the new approaches. Traditional anti-virus providers are adding next-gen capabilities, while the next-gen vendors are including signature-based protections in their suites. And, businesses are increasingly expecting to see anti-virus protection included in their security suite adoptions. As a spokesman for Malwarebytes said, "Businesses don't like to mix and match. They prefer to have one vendor to go to. So, the security solutions have multiple layers with multiple technologies involved to maximize the amount of protection."

According to a Ponemon survey, 64% of companies have experienced one or more endpoint attacks that compromised assets or infrastructure this year. And, 63% said the number of attacks is up compared to last year. The average cost of a successful attack has increased from $5 million to $7.1 million, with an average cost per compromised endpoint of $440. For small and medium businesses, the average cost was even higher, at $763 per endpoint.

Security experts are worried that organizations are moving too slowly in response to these new attacks and need to adjust their security strategies, getting over the mindset of just "guarding the perimeter and stopping what has been seen before" as one security company puts it.

This is why SIM2K has strengthened our malware protection offerings beyond just our SIM2K® MAVerick anti-virus protection. While this is still our standard installation as that first line of defense, we have other tools such as Cylance Protect that offer that next-generation security protection. Cylance will defend against zero-day attacks, or those malware injections that use non-traditional means to infiltrate your network. It also protects against Ransomware such as WannaCry and NotPetya, two that were in the news this past year. Cylance Protect provides endpoint utilizing AI driven technology to prevent attacks before they can damage your devices, network, or reputation.

Threats to your network, your data, your personal information, your banking and financial records and more are not going to go away. But, to be adequately protected, your company should be looking at maximizing the tools offered today. SIM2K will be glad to review your current status and make recommendations to improve your security profile. We have tried to implement MAVerick and Cylance for our Serenity and Pinnacle clients, but it never hurts to take a moment to review and make recommendations for improvements. Call us for more details.

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