Q-News

December 2021

A Word from Jack

As we wrap up our final newsletter of the year, for me, this is a time of reflection. What we did well, what we can improve, and focus on all the things we have to be grateful for. We are now about 21 months into the new reality of the pandemic. Things could have gone many ways. I am grateful to all our wonderful employees. They hung in there with us and allowed us to take care of our clients. I am grateful that the majority of our clients are still strong and continue to successfully navigate through these trying times.

As we move into 2022, a key initiative is to continue supporting the Microsoft 365 platform. Microsoft continues to improve and bundle more security features into their platforms. Their goal is to make the overall network (workstations, servers and connectivity to resources) more secure and manageable. This is especially important as the world goes to more of a work from anywhere model.

In closing, again a Big Thank You to our employees and customers. I wish everyone a happy and healthy holiday season and a successful 2022!

Where Cybersecurity Breaks Down

We already know Phishing accounts for more than half of ransomware attacks. A new study from Bitdefender reveals poor online habits prevail after a year of cybersecurity in the news. The first topic the study explores are passwords. They found over half of users memorized their passwords, and only 24% used a password manager. This data point can be tied to another later in the report on password reuse. The study found 22% of respondents use a single password for all online accounts. Less than half of users reported they use a different password for each account.

The study cited mobile threats as the new leading threat vector. Almost a quarter of users access a personal account with a work device. A mobile phone is the primary means of using the internet for half of users. We know smishing is up 300% over last year, and users are reporting the uptick. The study shows 61% of users reported scam messages or phishing over the past year. To add to the mobile threat, 30% of users are using a simple password like "1234" or are not locking their device at all.

Users were also asked about the kind of access children in their home had on internet devices. In the US almost half of children have full access to browse and install apps on mobile and desktop devices. The youngest demographic surveyed (18-24) were more likely to share information online and were generally less worried about online threats.

Criminals are exploiting the trust we had in text messages for two-step verification and appointment confirmations. The increase in SMS Phishing or Smishing makes business tools more vulnerable and hinders legitimate businesses from using text messaging as an advertising tool. Businesses need to understand how their corporate tools are being used outside the office in order to protect customer data.

Quanexus™
571 Congress Park Dr.
Dayton, OH 45459
937.885.7272
quanexus.com

Smishing Threat to Business Owners

Phishing using text message, or smishing (SMS phishing), saw a huge increase over the first half of the year. The increase is attributed to many people shopping from home in 2020, and companies using text messages for confirmation and to communicate with their customers. Smishing messages normally appear to come from banks, Amazon, mobile phone providers, or government agencies. Criminals use stories in the news to form their tactics like fake messages related to COVID contact tracing or messages from the government about tax returns.

Criminals are getting smarter and targeting smishing campaigns now include using the target's real first name, and phone or bank service they actually use. With so many data breaches recently, criminals are finding it easier to get their hands on more information about an individual and target them in a convincing way. Smishing numbers are up 300% in the US and 700% in the UK.

Corporate IT leaders are concerned about the implications of the increase in attacks on employee smartphones. As an industry, we've gotten very good at protecting computers on the business network, but many employees are working from home on consumer-grade networks and using personal and corporate smartphones on a variety of unsafe networks. Hackers targeting employees for business credentials with smishing is the logical next step in these attacks.

Steps to avoid becoming a victim

As with many of these threats, educating your employees is the first step. The messages almost always have a link to click on that's trying to steal login or personal information. Employees should know never to click on links in a text message or email and provide any kind of information. The text messages are designed to create urgency. They may say an account has a negative balance, or you just won a prize for paying your cell phone bill on time. The second step is to make sure the education sticks. Use an external IT company like Quanexus to test security awareness. Employees need to be able to recognize a suspicious message in the wild.

SMS Phishing is Evolving

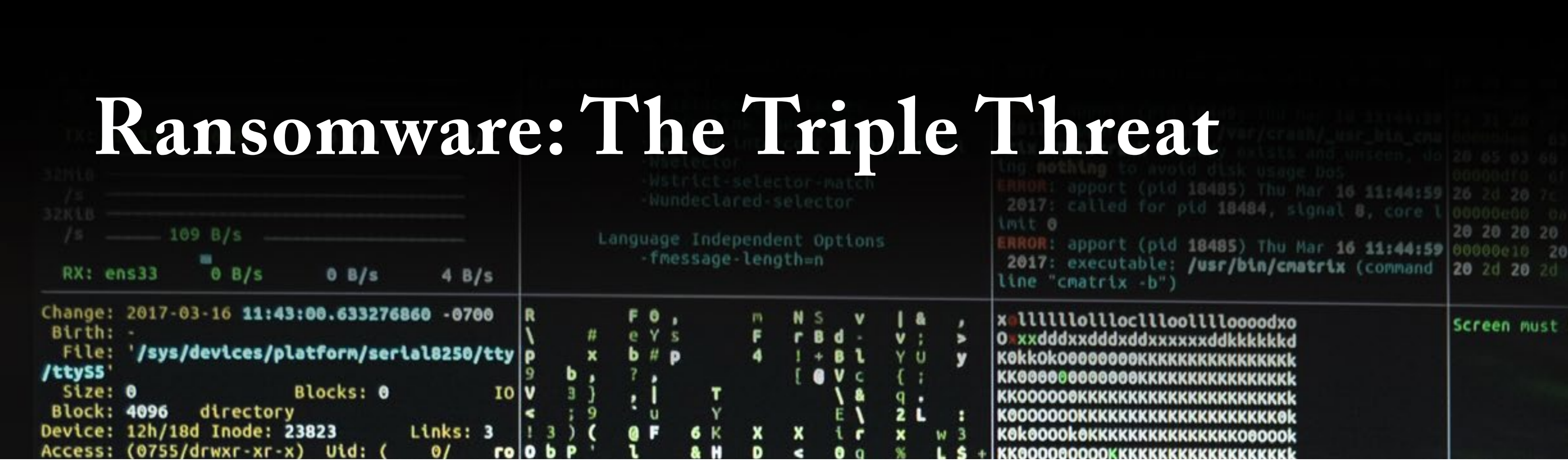
SMS Phishing or Smishing attacks have skyrocketed over the past two years. Attacks were up 328% in 2020, and recent data shows this new favored form of attack is up 700% in the first six months of 2021. Consumers have gotten used to businesses texting confirmation codes, special offers, and even medical appointment reminders. Most users do not have their guard up for phishing attacks over text message like they do for email. Criminals have been taking advantage of this oversight and collecting personal information or login and password credentials for everything from online banking to Amazon. A popular tactic might say something like, "Amazon detected a sign-in from a new device, was this you? If not click on this link to verify your account details." Users who are not aware of this new tactic would click the link and give the criminals their Amazon user and password.

However, there is a new evolved version of this attack vector. Users are being educated not to click links in text messages any longer, so criminals are moving away from the link and asking for a response instead. A recent report from Krebs on Security cited a user who received a professional looking text message that appeared to come from their bank. Instead of a link, the message asked for a response. When the user responded the criminal called them from a number that looked like a Chase bank number.

The user reported the operation was very smooth. The caller ID said J.P. Morgan Chase, and the scammer sounded professional and convincing. Luckily the user paused and told the scammer she would hang up and call the bank back. When she called back Chase said they had not called her or detected the payment alert shown in the text.

Luckily this user remembered the golden rule, "When In Doubt, Hang up, Look up, and Call Back." The same principle works to avoid phishing scams over email. Phishing attacks are designed to evoke emotion. The criminal wants you to move quickly before you have time to think through the steps. Criminals are looking for new and more convincing ways to steal personal information every day. As we move into the holiday shopping season, it's important to stop, hang up, look up the corporate phone number, and call the company directly.

Ransomware: The Triple Threat



When you think about ransomware, the first thing that comes to mind is the encryption of your files and data. The encryption process makes your files and data inaccessible. You then have three options: pay the ransom and hope you get your data back, restore your data from a good backup or suffer with the loss.

The options mentioned above are the single threat ransomware poses that most of us think of, but criminals are taking advantage of the data they steal and using it to threaten victims.

The New Triple Threat:

The triple threat applies more for businesses. It includes two more options that criminals may use to extort money from you. The second level of extortion is for the criminal to threaten the sale or release of your data on the public or dark web. Releasing the data on the public web would cause the company extreme embarrassment. The dark web would be used for the criminals to sell your data.

The third level of extortion is threatening to use the stolen data to perform targeted attacks against your customers.

Traditional thinking was, by backing up your data and creating a recovery environment, you will be much less vulnerable to the threat of ransomware. Backing up is still an excellent practice, but more focus needs to be placed on avoiding ransomware and data breaches.

The best way to avoid this kind of incident is through the implementation of a layered security approach, often referred to as a security stack, and continuous end user training.

Largest DDoS Attack on Record

The St. Louis Post Dispatch reported a flaw in a Missouri state website maintained by the Department of Education. Reporters for the newspaper discovered teachers' Social Security numbers were embedded in the source code of a web application that allowed the public to search for teachers in the state. The Post Dispatch warned the department of the vulnerability and waited for them to take it down before reporting on the issue.

Governor Mike Parson condemned the newspaper for their action and promised legal action against the reporters and the newspaper itself in a press conference after the reporting was made public.

"This administration is standing up against any and all perpetrators who attempt to steal personal information and harm Missourians," Parson said. "It is unlawful to access encoded data and systems in order to examine other peoples' personal information. We are coordinating state resources to respond and utilize all legal methods available."

However, the cybersecurity community has a different view of the vulnerability. The newspaper warned the Department of Education of the vulnerability and held the story until the data was offline. The Social Security numbers were found in the HTML of the site, meaning they were available to anyone with a web browser. Additionally, the Governor's comments could discourage future individuals from reporting a vulnerability.

The Missouri State Auditor found numerous issues with the state's cybersecurity practices. The report dated October 2021 cited issues with weak and shared passwords, backups not being stored securely, and system access that continues to be open to former employees.

State and local governments are in the cybersecurity news often for breaches. Typically, the report after the breach shows numerous security failings. Poor password practices, unused systems being left online, and unprotected backups are patterns we have seen before.

Instead of owning the problem, the school board is looking to place blame on the media. The media handled this correctly. The school board should be focused on fixing their issues and protecting the identity of their teachers. This should serve as a lesson for others to strengthen their cybersecurity practices.

Lessons from Large Data Breaches

There were more data breaches in 2020 than in the 15 previous years combined. The pandemic in the news, employees working remotely, and criminals following the money were all factors in the increase. Large data breaches in the news also forced businesses to revise their cybersecurity budget. Spending on cybersecurity grew 10% in 2020, spending on cloud infrastructure was up 33%, and notebook PC shipments were up 17%.

Research into the breakdowns from large breaches revealed people are still the problem. Phishing was the leading attack vector by more than two and a half times the next leading vector, malware. According to the FBI, there were more than 241,000 reported phishing victims in 2020. Criminals use phishing to steal PII, or financial information, but businesses owners are concerned with login credentials.

Hackers use stolen credentials to access web applications or databases where they steal and encrypt customer information, proprietary business strategies, or even government information. They get the login credentials largely through phishing attacks on employees.

However, Phishing attacks can be prevented through training and testing. A recent study ran a simulated phishing attack on two companies. The first provided annual security awareness training since 2016, the second did not have an awareness training program. The first company had one person click a link in an email. The second, without the cybersecurity awareness training, saw 7% of users click the malicious link.

The breakdown is getting federal attention. Carole House, the director of cybersecurity for the National Security Council said, "For too long, both public and private sectors have failed to take the necessary steps to implement basic cyber hygiene practices and cybersecurity defenses." She highlighted poor cybersecurity practices from individual companies to software developers. "Whether government, large corporations, small companies, or critical infrastructure, all of us can be targets of malicious nation-state or cyber-criminal actors," House said. "More importantly than just being a target, everyone has a role and a responsibility to defend against these threats. So, these partnerships between public and private sectors are only growing more critical to the safety of our nation in cyberspace."

Podcast

We have two new short Podcasts out this month. Jack and Chuck discuss MFA or Multi-Factor Authentication, and The Triple Threat of Ransomware!

Multi Factor Authentication - MFA

**Click Here for Podcast-
Multi-Factor Authentication**

Ransomware - The Triple Threat

**Click Here for Podcast-
Ransomware
The Triple Threat**

Quanexus™

**571 Congress Park Dr.
Dayton, OH 45459
937.885.7272
quanexus.com**

Follow Quanexus on Social Media!

Find Quanexus on Facebook, Youtube, LinkedIn, and Instagram! Click on the buttons below to access our social media pages. Like, comment and subscribe!

Also, subscribe to our email list to regularly receive tech news, cybersecurity alerts, and information on upcoming events. **Visit Quanexus.com to sign up!**

@Quanexus571 **@Quanexus** **@Quanexus** **@Quanexus571** **@Quanexus571**