Q-News

March 2021

A Word from Jack

As security breaches increase at an incredible rate, the basics remain the same. Last month we saw the SolarWinds breach, which was incredible. Along with SolarWinds, FireEye, Qualys, were also breached. What is significant about FireEye and Qualys is they are both security type companies. FireEye develops tools to monitor and protect the network. They have a significant amount of proprietary information that can be used to attack other organizations. Qualys on the other hand, produces a high-end network scanning and vulnerability tool. The reason behind the SolarWinds breach has been tracked back to an easily guessable password used on one of their development sites. While we see big companies getting hacked and breached, it all comes down to the basics: good passwords, multifactor authentication, and applying security updates to systems and applications. While there are no guarantees, the basic principles of network security keep smaller organizations from becoming victims.

We cannot absolutely protect ourselves from an incident that could result in a loss of data. It is vitally important organizations have a rock-solid backup solution so they can recover from the loss of data. Organizations should also have an incident response plan and be ready should something unexpected happen. At Quanexus we do our best to help our clients stay protected.

SolarWinds Back in the News

Executive leadership from SolarWinds testified to House Committees on Oversight and Reform and Homeland Security last week. The hearing revealed some new information on the attack we had not seen before. First, the breach was traced back to a weak password created by an intern. The password 'solarwinds123' was used to protect a server at the company, and then was posted publicly on June 17, 2018.

"…they violated our password policies and they posted that password on their own private GitHub account," former CEO Kevin Thompson said. "As soon as it was identified and brought to the attention of my security team, they took that down."

Lawmakers did not hold back their opinion on the password failure. "I've got a stronger password than 'solarwinds123' to stop my kids from watching too much YouTube on their iPad," said Rep. Katie Porter. "You and your company were supposed to be preventing the Russians from reading Defense Department emails!"

A researcher communicated with the company in 2018 and showed how he could access and move files onto the server at that time. The company did not correct the issue until November of 2019, so the password was public, and the server was accessible for almost a year and a half.

In addition to the password failure, NASA and the FAA were added to the list of government agencies infiltrated by the hackers. This brings the list of breached agencies to nine: Departments of State, Justice, Commerce, Homeland Security, Energy, Treasury, the National Institutes of Health, the National Aeronautics and Space Administration, and the Federal Aviation Administration.

The digital forensic team identified at least 100 private sector companies also breached. "In addition to this estimate, we have identified additional government and private sector victims in other countries, and we believe it is highly likely that there remain other victims not yet identified, perhaps especially in regions where cloud migration is not as far advanced as it is in the United States," Microsoft President Brad Smith said during the hearing.

Quanexus™

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

Insider Security Threats

An insider IT Security threat refers to a security risk originating inside an organization. The long term shift to a remote work environment increased insider threats dramatically last year. An insider security breakdown falls into three categories. The largest security threat comes from employee neglect or error at 61%. Attacks with stolen credentials are also considered insider threats, but malicious insiders make up 14% of insider attacks. These are employees who are knowingly downloading or distributing proprietary company data for profit or gain.

Malicious insiders act for various reasons, but the top of the list is money. A 2020 Verizon breach investigation report showed malicious insiders sold data for money, attacked their company for revenge, or in some cases were malicious just for fun. Many employees download privileged information before leaving or after being dismissed from a job. Surveys show in some industries this practice occurred almost 50% of the time.

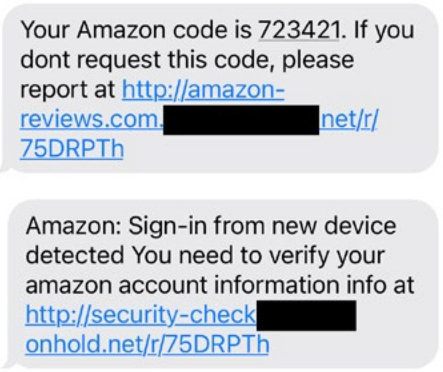
The other main category of insider threats is employee neglect. In this category employees are mishandling company data either because they didn't receive correct training, or because it's easier not to follow policies and controls. Working from home has exacerbated the possibility of abusing company data in this category. Some examples of data misuse are forwarding privileged data to a personal email address and printing privileged data to a personal printer. These are issues that an office firewall and document destruction policy were able to reasonably control in the past, but remote work is making the job more challenging.

There are steps business owners can take to protect against insider threats. Training is at the top of the list. Many employees in the 'neglect' category are there because of a lack of training. A business owner must have clear policies and controls and communicate them often. Another simple step is to follow the principle of least privilege. Employees should only have access to the data they need to perform their job function. Remote work and the move to cloud collaboration tools has opened up many employees to data they did not have access to in the office.

What is Smishing?

Smishing is a form of Phishing over text message or SMS message. The criminal's goals are the same as they are in typical Phishing attacks. Hackers are either trying to get you to divulge a username and password, install malware on your device, or convince you to send them money. There are numerous reasons criminals are using text messages instead of email for these attacks. First, the read and response rate is much higher in text messages. 98% of text messages are read, as opposed to only 20% of emails. Additionally 45% of text messages are responded to compared to only a 6% email response rate. Another reason for the shift is most consumers do not have their guard up against questionable text messages. Most technology users understand clicking a link in an email could be falling into a trap, but we don't have the same suspicion around text messages yet. A third reason is many reputable websites use SMS for two-factor authentication.

I received two Smishing messages attempting to look like they came from Amazon.



Your Amazon code is 723421. If you dont request this code, please report at http://amazon-reviews.com.[redacted]net/r/75DRPTh

Amazon: Sign-in from new device detected You need to verify your amazon account information info at http://security-check[redacted]onhold.net/r/75DRPTh

Just like typical Phishing emails, the text messages are designed to create urgency. The first message looks like a two-factor authentication message. Since I wasn't trying to log into my Amazon account at the time, the message makes me think someone else is trying to log into my account. There were a few things that made me pause and not click on the link, however. First the message came from a phone number, and not in the typical chain I get two-factor codes from Amazon in. The other 2FA codes I had from Amazon were all in the same text chain and did not have a link associated with them. Also, the more I looked at the message I noticed the odd grammar, and "don't" was missing an apostrophe. I received the second message five hours later. This message is supposed to create more urgency. Notice the end of the URL is the same random numbers and letters. Also notice there should be a period after "detected" and Amazon would probably capitalize their company name in correspondence.

Criminals are finding new ways to steal information and money. The technology industry is slowly moving away from SMS authentication to more reliable sources. Read our blog on Microsoft's stand on SMS authentication Here. Continue to be vigilant and suspicious of links you click on, even in text messages.

SECURITY ALERT

Public Employee Information Impact

Is it Safe to Have Information About Key Employees on Your Website?

Personally Identifiable Information (PII) is any information that can be used to identify an individual. We can divide PII into public and non-public information with some points that fall into a grey area. Obviously private PII are things like Social Security number, Drivers License number, credit card information, medical records. Public PII is information that can be accessed from public records. Examples of public PII are zip code, race, gender, date of birth. It is important to note that publicly available PII can be used in combination with PII found in a data breach or publicly posted by the individual to give the criminal a more complete picture of the individual.

Additionally, things get even more complicated and vary based on the industry or industries that you operate in. For example, in one industry there is a list of items that are considered PII. If any three of these items are listed together, it is considered protected PII. This can be as simple as a combination of first name, last name, and zip code.

Another category of PII is the data we use in public to conduct business. This PII includes name, email address, employer, position within company, and office address. PII in this category is considered sensitive but must be shared in order to communicate with others. There are security concerns when the data in this category is available publicly. Many small businesses have an "About Us" page where they share PII to help customers get to know the business and come across more personal. It is popular to share name, position within the company, a picture, and sometimes even the email address of the individual. While the intent is good, the information is available to the world, not just the potential customer base. This practice opens the employee up to more phishing attacks and gives criminals information they can combine with other publicly available PII.

Over the summer we covered the increase of new-hire phishing through LinkedIn. The professional networking tool is a great way to find new jobs and connect with other professionals. Unfortunately, criminals realized many employees were starting new jobs remote, and never met some of their coworkers. Hackers were taking advantage of new-hires and posed as the IT department of the new company. Criminals were able to gain access to internal network credentials by following publicly posted PII.

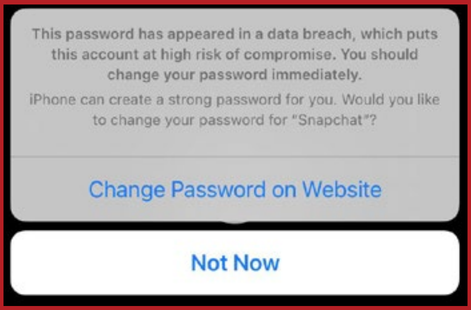
Be aware of your PII that is publicly available. This will help to recognize a phishing attack that may be using that data. We all must share some PII to exist and succeed in a business, but oversharing and making PII readily available sets users up to be a target.

A new practice is to not publicize key company individuals on the company's website.

New Focus on Password Security

Google announced a Chrome tool that will help manage passwords. Security breaches continue to be the result of poor password practices. Users continue to use simple passwords or use the same password for multiple services. We are seeing big tech focus on this human error issue like never before. Read more about it on the blog Here.

The new Chrome tool will allow users to update multiple passwords from one location. This is an improvement of the Safety Check tool they rolled out last year that enabled users to check the strength of a password, and alert users if a password had been found in a data breach. Apple has a similar password tool. iPhone users started seeing messages like these late last year.



This password has appeared in a data breach, which puts this account at high risk of compromise. You should change your password immediately.

iPhone can create a strong password for you. Would you like to change your password for "Snapchat"?

There are trusted password managers on the market, but a recent study showed only 12% of Americans were using one. We talked about protecting online identity and password managers in a recent podcast, you can see it here. For average tech users, a separate password manager often feels like one extra thing. Google says they have already seen 38% reduction of compromised passwords since the introduction of the Chrome tool late last year. These large companies are studying the habits of users and responding to the need.

Takeaways from Water Plant Attack

Hackers were able to infiltrate a water treatment plant in Oldsmar, FL on February 5th, and increase the levels of lye in the water to a dangerous level. Additional information has been released about the attack over the past week. We will explore why the Oldsmar water treatment plant is the definition of low hanging fruit for hackers.

An employee of the small municipal water treatment plant noticed their mouse moving around the screen independently of what he was working on. This was not uncommon because remote workers would often connect to the systems to make changes without communicating with the plant workers. The same employee noticed the mouse moving again five hours later, and then it changed the level of sodium hydroxide from 100 parts per million to 11,100 parts per million. At this level, the water is not safe to touch with bare skin, let alone drink. Luckily, the employee saw the change take place on his screen, corrected the change, and called the police.

Since the attack, we have learned more about the IT infrastructure of the water treatment plant. All the computers in the facility were running Windows 7 operating system. Windows 7 reached its end of life in 2020 and is no longer patched or updated by Microsoft. All computers were connected to the plant's supervisory control network, so all computers in the plant could make changes to the amount of chemicals in the water. All computers in the plant used the same password for remote access and were connected directly to the internet without a firewall between them and the outside world. The incident put other water treatment plants on high alert. The state of Massachusetts published a cybersecurity advisory for water treatment plants.

Small cities and municipalities can be easy targets for hackers because often their budget is not large enough to update systems regularly and keep an IT professional on staff. We reported on the ransomware attack on Lafayette, CO in September. They faced many of the same hurdles as the water treatment plant in Oldsmar, FL.

At Quanexus we use our Q-Stack to ensure clients are not easy targets. We can see the Oldsmar water plant skipped basically every step in the layered security approach we implement for our clients. For many small cities and businesses, a managed service provider can implement higher quality security for less than the cost of an additional employee.

Podcast

We have two new short Podcasts out this month. Jack and Chuck discuss current events in IT news on Virtual Bytes.

Virtual Bytes – Oversharing Information Online

Click Here for Vitual Bytes Podcast on Oversharing Information

Virtual Bytes - How you may be helping criminals attack your company – Part 2
Watch later
Share

Helping Criminals Attack your Company - Part 2

Click Here for Vitual Bytes Podcast - How you may be helping criminals attack your company

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