Texas Capital

Navigating the Cyber Threat

Today's Presenter: Casey Harris

CASEY IS A DIRECTOR AT **TEXAS CAPITAL** WITH 17 YEARS OF EXPERIENCE ACROSS A VARIETY OF CYBER SECURITY DISCIPLINES EXECUTED AT A GLOBAL SCALE WITHIN THE FINANCIAL SECTOR. CASEY BEGAN HIS JOURNEY IN SECURITY AT A NATIONAL DEFENSE LABORATORY, MOVED ON TO DIGITAL FORENSICS AT A BIG 4 ACCOUNTING FIRM, THEN TRANSITIONED INTO PROTECTING COMPANY AND CUSTOMER DATA WITHIN THE FINANCIAL SECTOR.

AT TEXAS CAPITAL, CASEY LEADS THE TEAMS THAT EMULATE THREAT ACTOR TECHNIQUES TO PROVIDE ASSURANCE THAT OUR TECHNOLOGY PLATFORMS ARE RESILIENT AGAINST THE TANGIBLE THREATS THAT EXIST IN CYBERSPACE.

Texas Capital Bank was founded to serve Texas businesses, their owners and employees. Texas Capital Bank is the only full-service financial services firm founded and headquartered in the State of Texas.

Table of Contents

Russia/Ukraine Conflict Cyber Update

Russia/Ukraine

Cyber Threat Update

On February 24, 2022, Russia launched an invasion of Ukraine, marking a major escalation of the ongoing Russo-Ukrainian conflict, which included numerous cyberattacks before and during the invasion — these Russian cyber-attacks continue.

- **2014–2021:** Crimea annexation — Ukraine is the perfect cyber sandbox for Russia.
- **Jan 13, 2022:** New destructive malware **"WhisperGate"** began attacking Ukraine.
- **Feb 18, 2022:** Large scale Distributed Denial of Service (DDoS) attack, Ukrainian Government networks and financial institutions.
- **Feb 23, 2022:** NATO-themed credential phishing attack; **"Cyclops Blink"** malware, and DDoS attack, Ukrainian Government networks and additional banking sites.
- **Feb 24–March 2022:** U.S. Treasury Notice of increased Russian cyber activity is expected; new destructive malwares **"HermeticWiper," "CaddyWiper"** and **"DoubleZero"** targeting Ukraine.
- **Late March 2022:** U.S. Courts approve FBI operation to enter undisclosed private U.S.-based devices to search for, remove Cyclops Blink, and change firewall rules to prevent future Cyclops Blink malware. Meanwhile, Russia takes down Ukraine's Internet in largest cyberattack to date.
- **April 8, 2022:** Russia attacks Finnish Government website with DDoS in retaliation for ongoing talks to join NATO, while Ukraine blocks destructive Russian malware **"Industroyer2"** from cutting power in unspecified Ukrainian region.
- **May 2022:** U.S. Cyber Command announces cyber support operations alongside Ukraine.
- **June 2022:** A few major U.S. Financial Institutions are hit with a targeted ransomware attack.
- **July–Dec 2022:** Continued coordinated cyberattacks against Ukraine tied to physical strikes.
- **Jan 2023:** Russian hacking team known as Cold River targeted three nuclear research laboratories in the United States this past summer, according to internet records reviewed by Reuters and five cybersecurity experts.
- **Early February 2023:** Pro-Russia hacktivists attack Western hospitals, including in the U.S.
- **Mid-February 2023:** Russian-developed "Chernovite" tried to take down industrial systems of electric and liquefied natural gas sites in the United States but was foiled by authorities.
- **May 9, 2023:** U.S. DoJ announced the disruption of "Snake" malware, an implant used for cyberespionage by Center 16 of the Russian Federal Security Service (FSB).
- **June–July 2023:** Pro-Russian hacktivist groups conduct DDoS attacks against Western financial institutions, including the European Investment Bank.

Russia/Ukraine

Our Thoughts on the Impact of the Russia/Ukraine War

- Russian disruptive or destructive cyberattacks may have contributed modestly to Moscow's initial invasion, but since then they have inflicted negligible damage on Ukrainian targets.
- Cyberattacks have neither added meaningfully to Russia's kinetic firepower nor performed special functions distinct from those of kinetic weapons.
- Intelligence collection — not cyber effects — have likely been the main focus of Russia's wartime cyber operations in Ukraine, yet this, too, has yielded little military benefit.
- While many factors have constrained Moscow's cyber effectiveness, perhaps the most important are inadequate Russian cyber capacity, weaknesses in Russia's non-cyber institutions, and exceptional defensive efforts by Ukraine and its partners.
- As the war continues, Russian intelligence collection probably represents the greatest ongoing cyber risk to Ukraine.
- We do not foresee any fallout from this conflict on the U.S. Financial Sector or TCB.
- Other countries, such as China, have been watching closely and may conduct similar activities in the future (e.g., China against Taiwan) — Future of Warfare.
- Criminal cyber organizations/gangs have not been deterred by the war, and in fact are emboldened — they still represent the greatest threat to the U.S. Financial Sector.
- 2023 saw a slight decrease in ransomware attacks, but an increase in ransom amounts ($).
- The U.S. & Global economy influence corporations' desire to invest in cybersecurity.
- Cyber gangs have had no slowdown in pursuing their ill-gotten money.
- 2022 witnessed an increase in digital customer shopping/banking — 75% of all customer interactions are online (Deloitte).
- Customers are more inclined to want a secure onboarding process (67%) over a good customer experience.

Texas Capital Preparation for Russian Cyber Fallout

MARCH 2022

U.S. GOVERNMENT LAUNCHES "SHIELDS UP" CAMPAIGN TO PREPARE

- Texas Capital took significant actions to reduce threat exposure/risks and accelerate network security protocols.
- Aggressively increased patching, accelerated deployment of security tools, increased data loss protection protocols, increased threat monitoring and response capabilities, and worked with critical partners to block access from numerous countries.
- Firm implemented Cyber Threat Conditions as a measure to risk exposure to the internet:
  - Reduced access to the internet and blocked countries accessing Texas Capital

CISO WATCH ITEMS

- Runaway destructive Russian malware across globe specifically targets U.S. Financial Sector.
- Physical Russian conflict spills over to NATO.

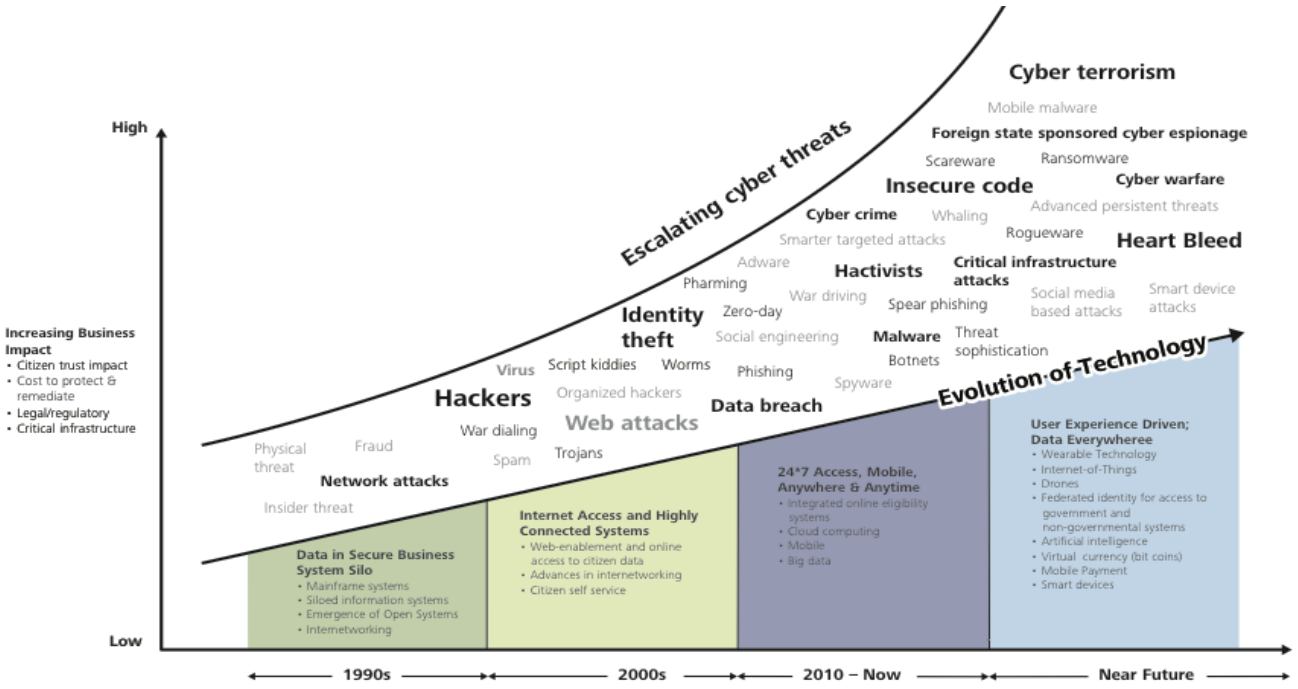
NEXT STEPS

- Continue to harden the Texas Capital network while tuning security controls.
- Remain vigilant! Continue close engagements with our Security partners.

Global Cyber Intel Update

The Evolution of a Cyber Threat = Very High Risk

Evolving technology and rapidly escalating cyber threats call for a deliberate approach to make commanding progress.



Source: Reproduced from the 2014 Deloitte-NASCIO Cybersecurity Study
"State governments at risk: Time to move forward"

U.S. CYBER BREACHES

Q3 2022

- Marriott (seventh time)
- Twitter
- Uber
- Twilio
- Cisco
- Plex
- LastPass
- DoorDash
- Samsung
- TikTok
- IHG/Holiday Inn
- American Airlines
- Verizon
- Bed Bath & Beyond
- Amazon
- Dropbox
- LastPass (second time)
- Okta

Q1 2023

- T-Mobile
- ChatGPT
- Chick-fil-A
- Activision
- Google Fi (via T-Mobile)
- MailChimp
- Norton LifeLock

Global Cyber Threats

CYBER THREATS ARE INCREASING IN FREQUENCY & SOPHISTICATION

- **Cyber Crime = a $6T industry** that is reinvesting in itself and commoditizing services (e.g., Ransomware as a Service); result = lower bar for entry for new threat actors
- Impact = Business Shutdown, Data Exfiltration, Extortion, Regulatory Fines, Reputational Damage
- Risks = Very High (Operational, Regulatory, Reputational, Legal, Financial)

THREAT ACTORS

- State Actors (Advanced Persistent Threats — APTs)
  - Motivated by espionage and setting the conditions for or as part of physical conflict
  - **Russia:** Focusing on national governments and a wide variety of industries; supporting the Ukraine ware effort.
  - **China:** Focusing on intellectual property theft and economic influence.
  - **North Korea:** Motivated by espionage and sanctions evasion; financial institutions are major target for intelligence and monetary gain.
  - **Iran:** Highly interested in destructive capabilities.
- Criminal Organizations
  - Lockbit, Conti, Blackcat, Hive
  - Motivating by monetizing access and data
- Hacktivists
  - Anonymous
  - Motivated by causing virtual harm for reasons of political views, cultural/religious beliefs, national pride or terrorist ideology

Global Cyber Attack Vectors

ATTACK VECTORS | *The way a firm can be targeted*

- **Email Phish:** Malicious attachment and/or malicious URL (hyperlink)
- **Vulnerable Tech Environment:** Internet-facing website, improper cloud configuration, and vulnerable applications or technology
- **Third Party:** unsecured business-to-business connection or infected email
- **Supply Chain**: Solar Winds (malware inserted into third-party software/app that we use)
- **Insider Risks:** Employees or contractors intentionally or unintentionally stealing confidential or proprietary data

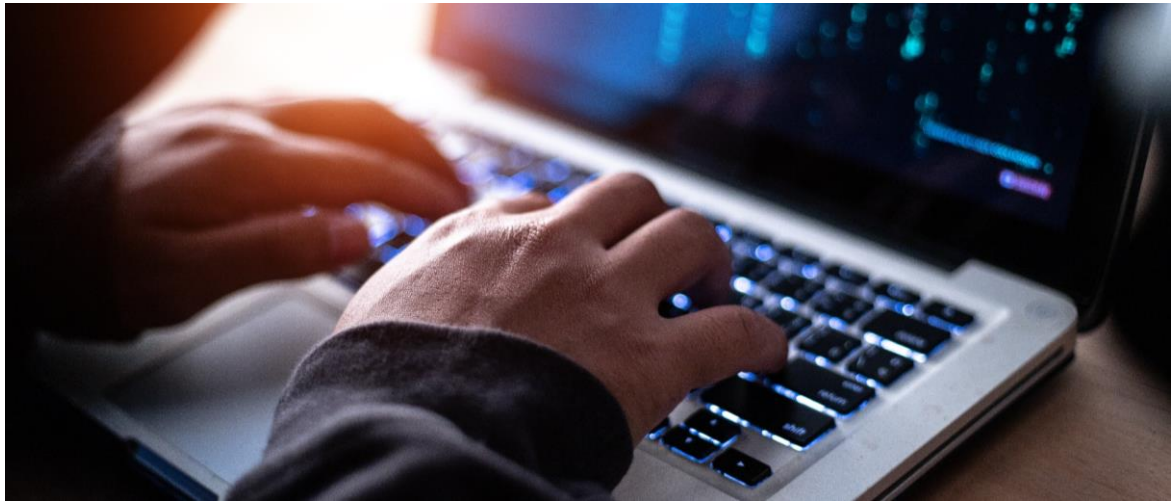
COMMON ROOT CAUSES

- Poor Cyber Hygiene
- Social Engineering Exploitation
- Immature Information Security Controls

According to Forbes, by 2025, 60% of firms will use cybersecurity risk ratings as primary determinant when choosing who they will do business with.

- Cybersecurity ratings will be as important as credit ratings
- Having a very good cybersecurity rating will be a business discriminator

Biggest Bank Robberies



MARCH 2022

BANCO CENTRAL IN FORTALEZA, BRAZIL

- Six to 10 robbers
- Dug a 256’ long tunnel from nearby building
- Drilled through 3’7” of steel and concrete
- Stole $69.8M USD in Brazilian reais notes weighing 7,716 pounds
- It took three months to dig the tunnel

2013–PRESENT

CARBANAK (AKA CARBON SPIDER)

- Wrote one banking malware Trojan called Carbanak while sitting at home drinking coffee
- Infiltrated over 100 banks and their ATMs in 40 countries
- Stole over $1.2B USD
- In 2018, three Ukrainian nationals were arrested…but there are probably more out there

Ransomware Stats, Costs & Consequences

PRIMARY CYBER THREAT = RANSOMWARE/MALWARE

- Ransomware attacks occur 19 times a second, on average, according to cybersecurity firm Astra.
- 2023 (year ending March 2023), it took an average of 204 days to identify a breach and an average of 73 days to contain.

AVERAGE COSTS OF A SINGLE RANSOMWARE EVENT

2023 (year ending March 2023)

- The Ransom = $0.5–$10MM (financial institutions tend to be higher).
- Business Impact/Cost to Recover Network = $5.90MM (Financial Industry, IBM Report).
- Cost per Record w/ Customer PII = $183*.
- Paying ransom led to negligible savings, if any, on average, as cost of payment not included.
  - Also, there is a higher chance of being targeted again.
  - And, threat actors may still dump/sell your data.
- Cyber insurance may or may not cover costs.

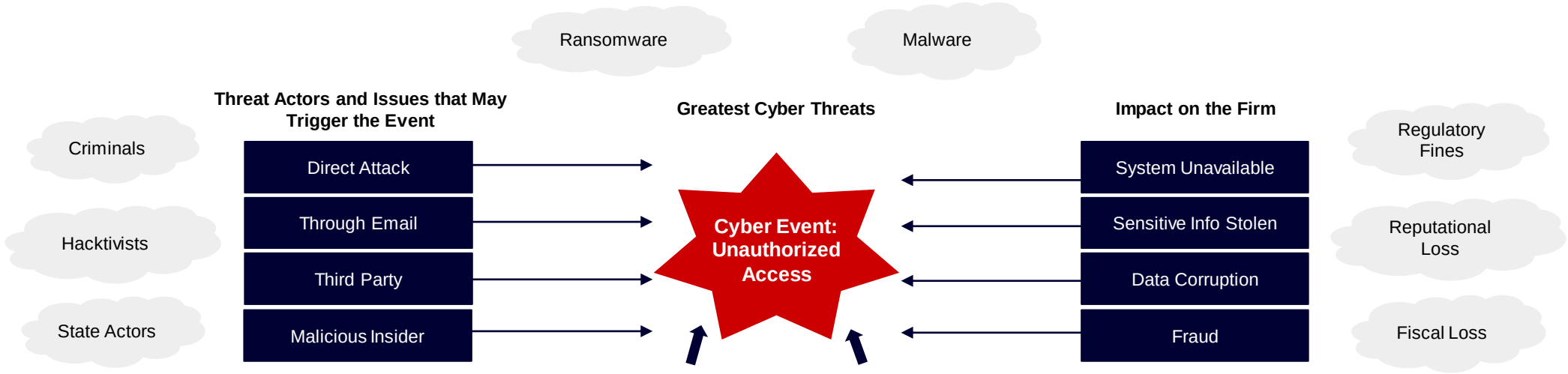
CONSEQUENCES

- Financial loss
- Reputational damage
- Operational downtime
- Legal action
- Loss of sensitive data

What is Texas Capital doing to navigate the cyber threat landscape?

Cyber Threat Landscape

Firm's Cyber Risk Management



Factors that Contribute to InfoSec Program Development

- The Firm Business Strategy & Rate of Change
- Customers & Clients' Perception
- Regulators
- Third Parties

ID, Prevent & Detect | Means to Respond, Mitigate & Recover

The Firm's InfoSec Program
Decrease Likelihood and/or Impact

Policy & Governance	3rd Party Cyber Risk	Network Security	Security Operations	Insider Threat Pgm
Risk Assessments	Vulnerability Mgmt	Data Security	Cloud Security	Threat Intelligence
Cyber Ed & Awareness	Access Mgmt	Application Security	Tech Architecture	Threat Emulation

Primary Functions of InfoSec Program

Focus Areas for InfoSec Program Development

- Layers of Security Across and Within Network
- Control Access Multi-Factor Authentication
- Robust Counter-Phishing Controls
- Robust Third Parties and Insider Risk Programs
- Robust Threat Detection and Incident Response Capability

How is Texas Capital different?

"Most Trusted Bank in America"
(*Newsweek* — Mar 2022)

We are a leading player building a Texas-Based Collective Defense initiative

- Partnering with major security firms to develop and implement

Size Matters
Large enough to attract best talent; small enough to be nimble to rapidly deliver Best-in-Class cybersecurity

"A" Score on Security Score Card
(Cybersecurity rating firm)

Strategy-Driven Leadership
Multiple sectors perspective

- Large Financial, U.S. Government & Healthcare Sector leaders (USAF, BofA, JPMC, Goldman Sachs, Regions, Abbott, Tenet, Law Enforcement, NSA)
- Balance: Risk-Based, Information Technology, Cyber Operations, Business-Focused

Support and Resources from the Board and C-Suite

- Great risk-and-security culture and focus to allow an enterprise-wide adoption of cybersecurity
- Client-Obsessed — Numerous new banking initiatives centered on technology-driven solutions to improve user experience and customer options
- Client engagement events to promote security

What Do We Do for Our Clients' Cybersecurity?

Login Security

Secure Online Messaging

Security Alerts

Money Movement Approvals

Anti-Fraud Solutions

Branch & Office Security

Offer Resources for Customers

What can you do to improve cyber hygiene?

The Human Element of Information Security

Phishing

Phishing is when **an attacker masquerades as a reputable entity or person** in email or other forms of communication. Attackers will commonly use phishing emails to distribute malicious links or attachments that can perform a variety of functions.

82% of breaches involve a human element. Part of our defense for this is regular simulated phishing campaigns to increase awareness and provide real-time training if a user doesn't catch the phish.

How to Detect a Phish

Phishing Test for the Week of September 20, 2022

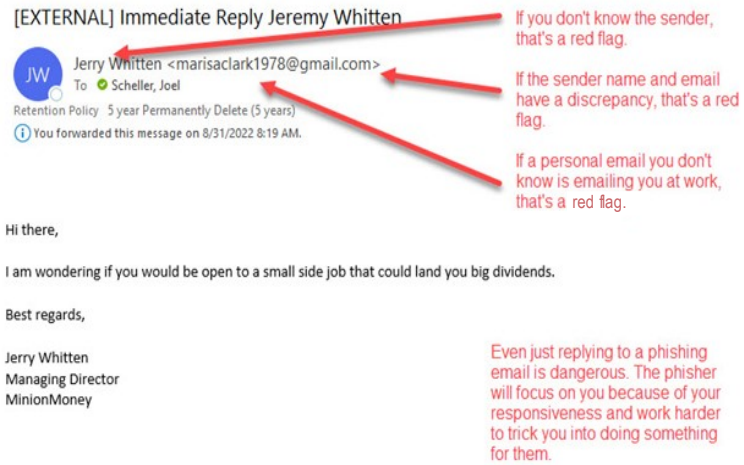
September 23, 2022 | 0 Likes | 0 Comments

There is good news and not-so-good news about our latest phishing test.

The good news is that with 2723 employees receiving the test, we had no one fail. That is very good news indeed! The test before this one, we had a success rate of 97.1%, based on 79 failures, which isn't bad; 0 failures is a whole lot better, though.

However, our reporting dropped to 31.6% from 34.6% from 42.9%, over the last three tests. Reporting suspicious emails is a very important part of exercising security awareness, so we would like to see the trend line slanting in the other direction. We depend on everyone to use the "Phish Alert" button in Outlook; It is a huge help in keeping Texas Capital Bank safe.

Check out the red flags in the last phishing test below:



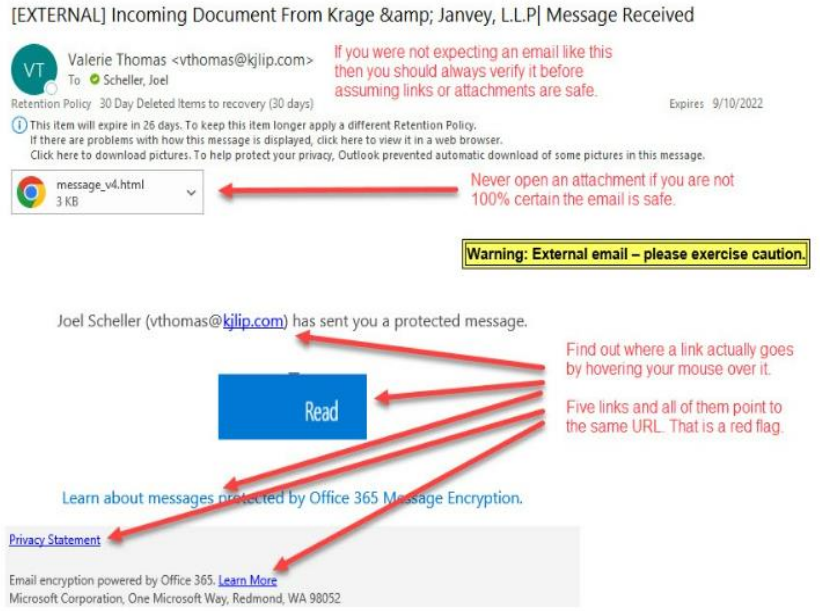
Phishing Test of Week August 11, 2022

August 11, 2022 | 0 Likes | 0 Comments

Of 2559 employees that received the phishing test, 114 failed it. That is a success rate of 95.5%. which is much lower than our last phishing test (96.4%).

The good news is that our reporting rose up to 42%. We depend on everyone to use the "Phish Alert" button in Outlook; it is a huge help in keeping TCB safe.

Check out the red flags in the last phishing test below:

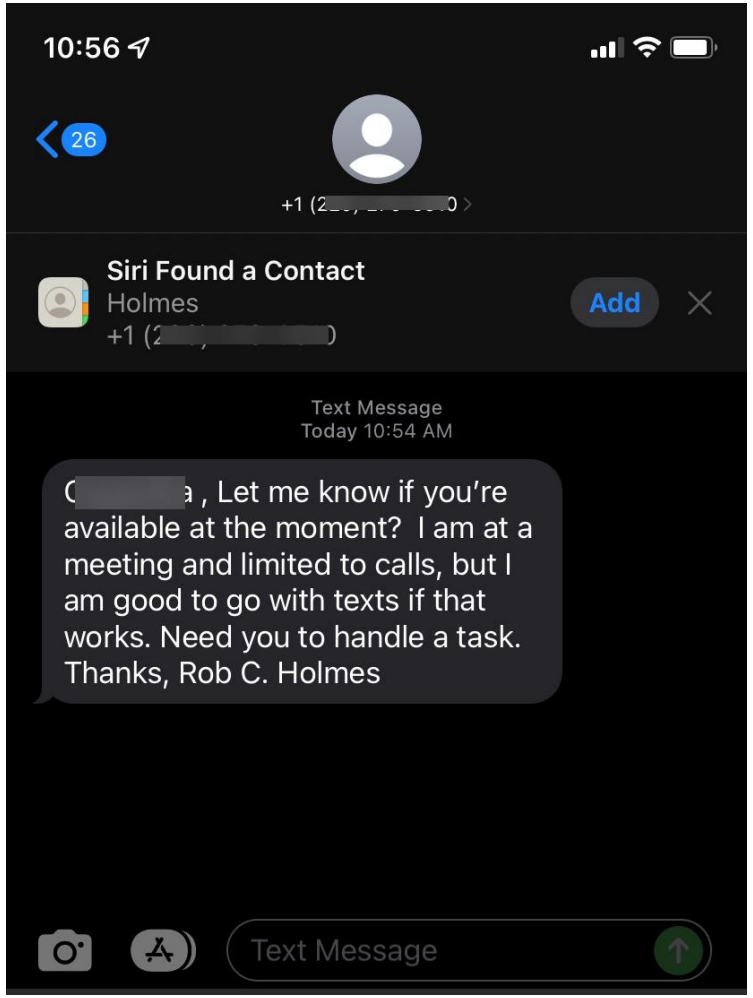


How to Detect a Phish | *Disinformation*

Check sources by using fact-checking websites and ask yourself these questions before you share any information.

1. Is the headline trying to cause a strong emotional reaction?
2. Is the author credible?
3. Is the date current?
4. Has the image been altered?
5. Are all the facts accurate?
6. Is the source of the information legitimate?

SMS Phishing (Smishing)



Attackers target employees by sending cellphone text messages that **appear to be from the CEO** or other executives of their company.

This type of initial phishing text message is usually **followed by an urgent request** for the recipient to complete an action that will result in a data breach or financial theft. The most popular ask is that the recipient purchase gift cards and text back the gift card numbers.

Good Personal Cyber Hygiene

Here is a personal cybersecurity checklist you can use proactively to make sure you are following best practices.

KEEPING PASSWORDS SAFE & SECURE

- ✓ I avoid using the same password for different accounts.
- ✓ I change my passwords on a regular basis.
- ✓ My passwords are at least 12 characters long (and ideally longer).
- ✓ My passwords involve a mix of uppercase and lowercase letters plus symbols and numbers.
- ✓ My passwords avoid the obvious — such as using sequential numbers ("1234") or personal information that someone who knows me might guess, such as my date of birth or a pet's name.
- ✓ I change the default passwords on my Internet of Things (IoT) devices.
- ✓ I avoid writing my passwords down or sharing them with others.
- ✓ I use a password manager to help generate, store and manage all my passwords in one secure online account.

USING MULTI-FACTOR AUTHENTICATION

- ✓ All my essential accounts — such as email, social media or banking apps — are protected with multifactor authentication (MFA), using an app like Google Authenticator or Authy.
- ✓ I save MFA backup codes in my password manager.

BACKING UP DATA REGULARLY

- ✓ I keep files secure and protect against data loss by backing up essential files offline, either on an external hard drive or in the cloud.

ASSESSING YOUR PERSONAL SOCIAL MEDIA FOOTPRINT & HABITS

- ✓ I don't post private information such as my home address, private pictures, phone number or credit card numbers publicly on social media.
- ✓ I have reviewed my social media privacy settings and made sure they are set to a level I feel comfortable with.
- ✓ I avoid quizzes, games or surveys on social media that ask for sensitive personal information.
- ✓ I am cautious about the permissions I accept for all the apps I use.
- ✓ I keep my computer and phone locked with a password or PIN.
- ✓ I take care not to disclose private information when using public Wi-Fi.
- ✓ I understand that using a Virtual Private Network or VPN — especially when using public Wi-Fi – helps to maximize my privacy.
- ✓ I make sure any online transactions I make are via a secure website — where the URL starts with https:// rather than http:// and there is a padlock icon to the left of the address bar.
- ✓ I share information about online privacy with family and friends to help keep them safe as well.

Good Personal Cyber Hygiene | *Continued*

KEEPING APPS, SOFTWARE & FIRMWARE UP TO DATE

- ✓ I update apps, web browsers, operating systems and firmware regularly to make sure I'm using the latest versions.
- ✓ Where possible, I have set up features to ensure automatic software updates.
- ✓ I delete apps I no longer use.
- ✓ I only download apps from reputable or official sources.

SECURING ROUTERS

- ✓ I have changed the default name of my home Wi-Fi/I have changed my router's username and password.
- ✓ I keep firmware up to date.
- ✓ I have disabled remote access, Universal Plug and Play, and Wi-Fi Protected Setup.
- ✓ I have set up a separate network for guests to use.
- ✓ I have made sure that my router offers WPA2 or WPA3 encryption to protect the privacy of information sent via my network.

AVOIDING SOCIAL ENGINEERING ATTACKS

- ✓ I avoid clicking on suspicious links or links I am not sure of. I avoid opening emails that look suspicious.
- ✓ I avoid downloading suspicious attachments from emails or text messages I am not expecting.
- ✓ I don't click on ads that promise free money, prizes or discounts.

USING NETWORK FIREWALLS

- ✓ I use a firewall to prevent malicious software from accessing my computer or network via the internet.
- ✓ I ensure my firewall is correctly configured.

ENCRYPTING DEVICES

- ✓ I encrypt devices and other media which contain sensitive data — including laptops, tablets, smartphones, removable drives, backup tapes and cloud storage.

WIPING HARD DRIVES

- ✓ Before I dispose of or sell a computer, tablet or smartphone, I make sure I wipe the hard drive clean to prevent any personal information from being accessed by others.

ENSURING HIGH-QUALITY ANTIVIRUS PROTECTION

- ✓ I use high-quality antivirus software that scans for and removes computer viruses and other malicious software.
- ✓ I keep my antivirus software up to date.

Ultimately, cyber hygiene means developing a protective routine to keep your personal and financial information secure when using your computer or mobile device. Using strong passwords and changing them regularly, keeping software and operating systems up to date, wiping hard drives, and using a comprehensive antivirus will help you stay ahead of the latest cyber threats.

Social Media Platform Threats

Fake Social Media personas are a common first step for criminals to social engineer their way into your organization or phish you.

What can you do to spot a fake?

- **Too-good-to-be-true credentials** — CEO sending an unsolicited connection request, especially to a new hire/intern
- **Sudden increase in number of invitations to connect** — a common tactic by criminals who are trying to gain access to you or your firm
- **Odd misspellings or incorrect capitalization** — usually means the criminal is rapidly creating multiple fake profiles
- **Only one job listing or very few existing connections** — rapid fake profile creation; account does not have realistic data, which is a sign of a phony persona
- **Profile picture looks too perfect** — picture looks suspiciously like stock imagery or has been artificially generated
- **Location does not match company** — profile says they live in Iceland but work in Silicon Valley
- **Education does not match work history** — dozen companies worked for but graduated college two years ago
- No recommendations or engagement within social media platform — probably not a real persona (harder to pick this one out)

What can you do?

Traveling

- Don’t use public Wi-Fi when accessing confidential info: use a personal hotspot instead.
- Keep devices secured and accounted for at all times.
- Disable automatic Bluetooth pairing.
- Don’t allow your devices to auto-join unfamiliar Wi-Fi Networks.
- Don’t use borrowed chargers or public charging stations.

Physical Security Reminders

- Never use unknown USB devices.
- Always lock your workstation.
- Keep confidential information secured — use privacy screens and headphones, if necessary.
- Implement a clean-desk policy by removing business documents, notes, etc.
- Don’t allow unauthorized individuals to tailgate into your organization.

Texas Capital

Questions?