The Cyber Threat 2021

Current Fraud Trends, Prevention, and Best Practices

Presented by: Mike Mason, *Assistant Vice President*
***e*-Payment Solutions Department**
First National Bank Alaska

Topics of concern

THREAT ENVIRONMENT

- Cyber crime economy
- Fraud as a service

CURRENT FRAUD TRENDS

- Email threats
- The “Internet of Things” or IOT
- Corporate account takeover
- Supply chain attacks and data breaches

PREVENTION

- Personal
- Business
- Passwords

BEST PRACTICES

Cyber crime economy

DARK WEB

Fraudsters and other criminals have migrated to the 'dark web' which is only accessible via TOR, a method of anonymous routing which allows for servers to hide from authorities.

CYBER CRIME FORUMS

The explosion of online cyber crime forums, particularly among Russian-language identity theft gangs, has resulted in a veritable gold rush of would-be fraudsters and scammers.

"Crime forums almost universally help lower the barriers to entry for would-be cybercriminals. Crime forums offer crooks with disparate skills a place to market and test their services and wares, and in turn to buy ill-gotten goods and services from others."

BRIAN KREBS | SECURITY RESEARCHER AND AUTHOR

Source: www.krebsonsecurity.com

Fraud as a service

HACKERS FOR HIRE

Organized crime rings allow for a diversity of services to be offered; hacking, money mules, and more.

BOTNETS FOR RENT

Compromised PCs and home network routers form distributed networks for custom attacks, spam, and espionage.

MALWARE BY LICENSE

Fraud packages include custom-tailored malware for stealing valid bank account credentials and login info.

Email scams

NIGERIAN PRINCE / 4-1-9 SCAMS
Advance fee fraud

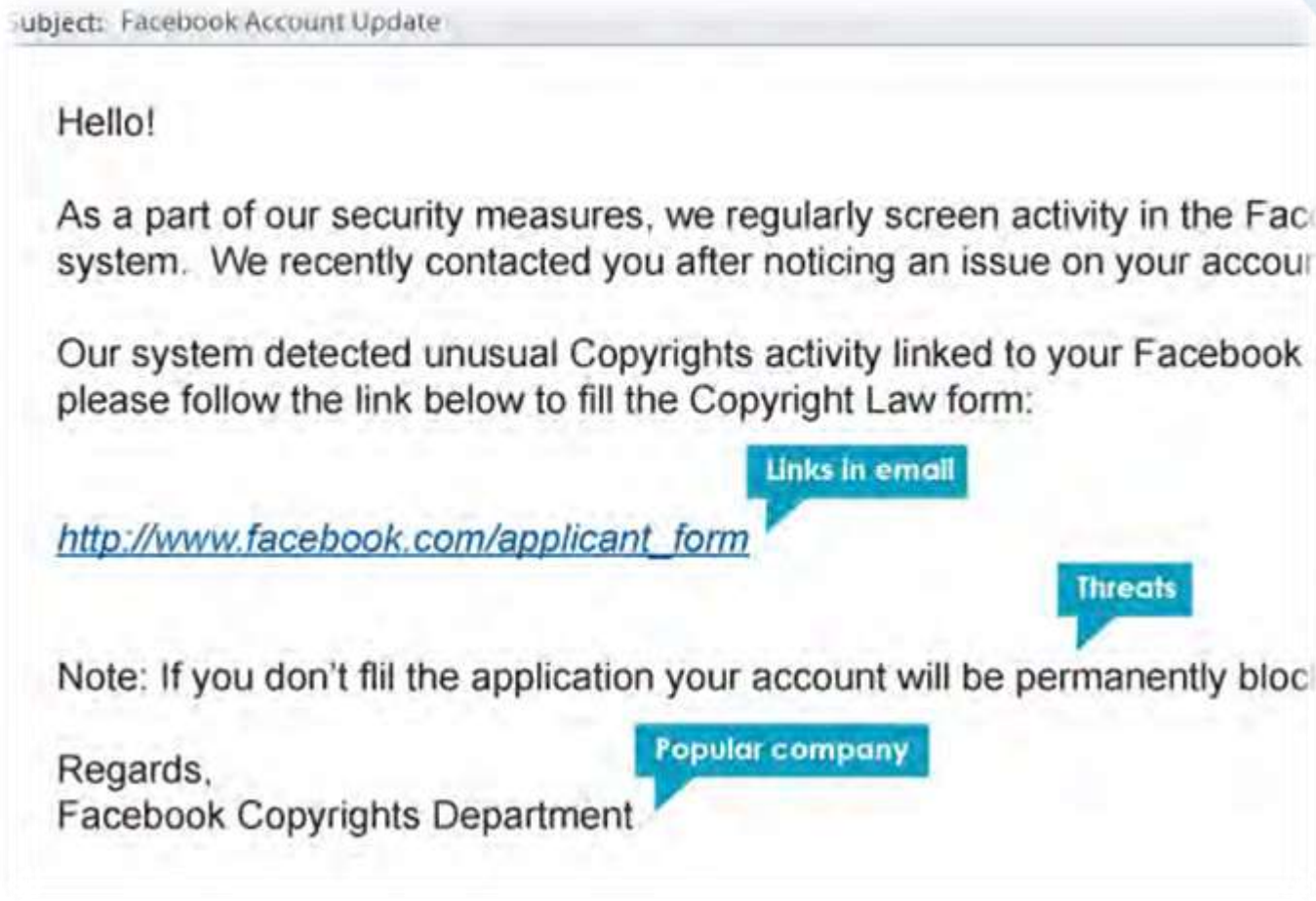
OVERPAYMENT SCAMS

DISASTER RELIEF SCAMS
Priority line for vaccine

- After nearly every major disaster whether it be from a storm, earthquake, or other event scammers will attempt to dupe people into sending them money. The coronavirus pandemic is no different. Fraudsters have already begun selling fake test kits, charging fees for “priority” access to the vaccine, among other schemes. These are typically email, telephone, and text messaging driven fraud campaigns targeting specific regions.

More info: https://www.ic3.gov/preventiontips.aspx

Phishing


ubject: Facebook Account Update
Hello!
As a part of our security measures, we regularly screen activity in the Fac
system. We recently contacted you after noticing an issue on your accou
Our system detected unusual Copyrights activity linked to your Facebook
please follow the link below to fill the Copyright Law form:
Links in email
http://www.facebook.com/applicant_form
Threats
Note: If you don't flil the application your account will be permanently bloc
Popular company
Regards,
Facebook Copyrights Department

Evolved email threat

Sophisticated Spear-Phishing Campaigns

PROFESSIONAL WRITING

New category of professional, well written, and effective attack emails.

REGIONAL TARGETING

Fraudsters working together to target industries and geographic areas.

PREMEDITATED SELECTION OF VICTIMS

Targeting employees within an organization who are typically able to make payments.

Spear phishing

Subject: employee making negative comments about you and the company

From: <name>@<compromised company's domain>

I noticed that a user named FinanceBull82 (claiming to be an employee) in an investment discussion forum posted some negative comments about the company in general (executive compensation mainly) and you in specific (overpaid and incompetent). He gave detailed instances of his disagreements, and in doing so, may have unwittingly divulged confidential company information regarding pending transactions.

I am a longtime client and I do not think that this will bode well for future business. The post generated quite a few replies, most of them agreeing with the negative statements. While I understand that the employee has the right to his opinion, perhaps he should have vented his frustrations through the appropriate channels before making his post. The link to the post is located here (it is the second one in the thread):

http://forum.<domain>/redirect.
php?url=http://<domain>%2fforum%2fequities%2f375823902%2farticle.
php\par

FIN4

- **Sophisticated spear phishing campaigns**
- **Stolen passwords to access webmail**
- **Traded on stolen M&A activity**

Source: FireEye – Hacking the Street

Business email compromise

BUSINESS EMAIL COMPROMISE

Type of fraud that involves what appear to be legitimate business email accounts

Fraudsters use compromised or spoofed email accounts to provide falsified wire transfer instructions, request private data, or they use malware to compromise the victim's network.

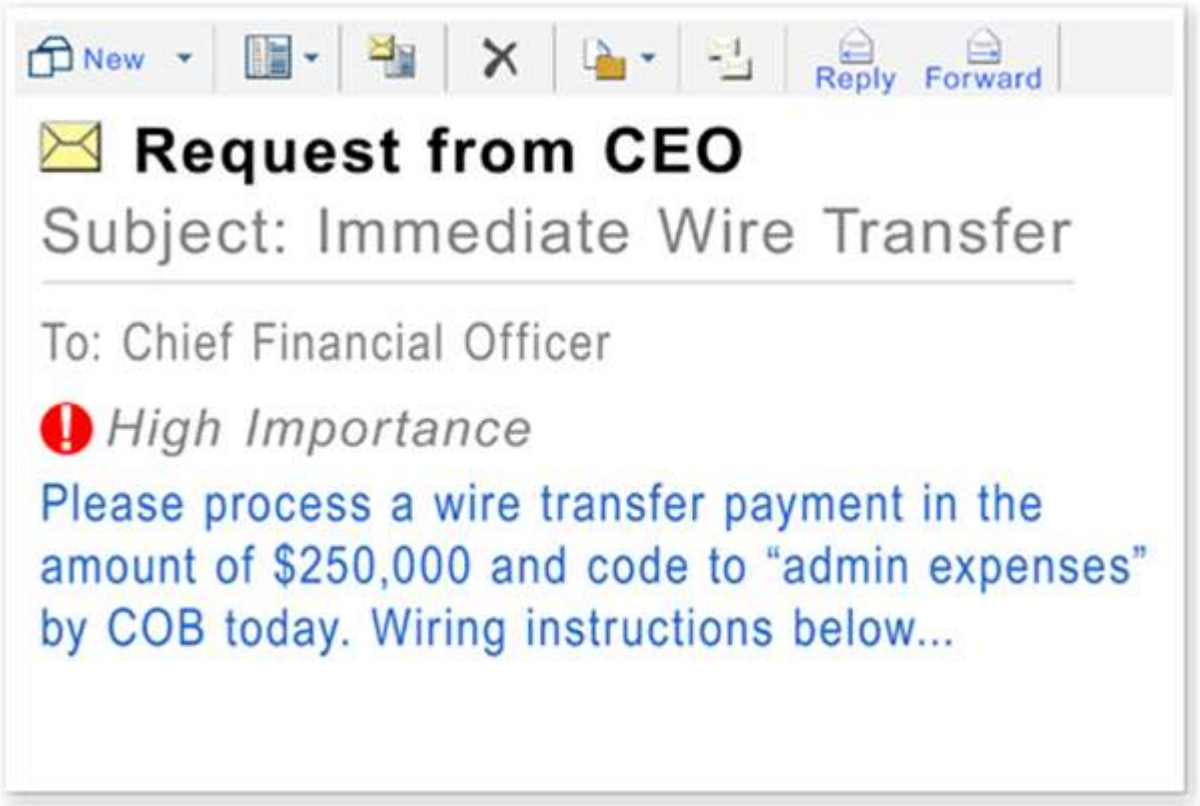
CHARACTERISTICS

- Targeted email "from" a trusted business contact requesting payment
- Typically contains element of urgency to apply time pressure
- Requests for secrecy are a major red flag

Business email compromise

Scheme: Accounts Payable / Invoice Fraud

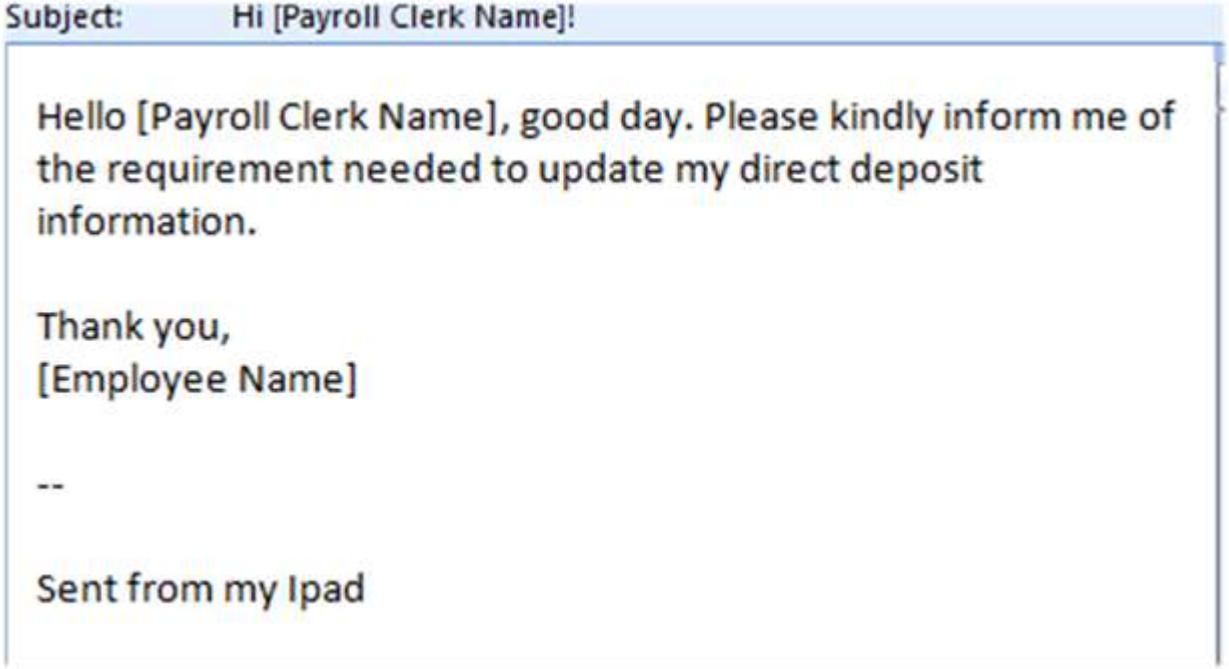
Target: AP Staff / Wires & ACH



Business email compromise

Scheme: Payroll Diversion

Target: HR Staff / Direct Deposit (ACH)



Source: www.ic3.gov FBI Public Service Announcement – September 18, 2018

Business email compromise

Scheme: Gift cards

Target: Employees / Corporate credit cards

New tactic sees a 1,240% increase between 2017 and 2018

- **Be mindful of any email, phone call or text messages requesting multiple gift cards even if the request is ordinary.**
- **Beware of sudden changes in business or personal practices and carefully scrutinize all requests for multiple gift card purchases even if requests are ordinary.**
- **Since many of the fraudulent e-mails reported in this new trend are spoofed, confirm requests for the purchase of gift cards using two-factor authentication. If using phone verification, use previously known numbers, not the numbers provided in the e-mail request.**

Source: www.ic3.gov FBI Public Service Announcement – October 24, 2018

Business email compromise

LOSS STATISTICS REPORTED TO THE INTERNET CRIME COMPLAINT CENTER & FBI

October 2013 to July 2019

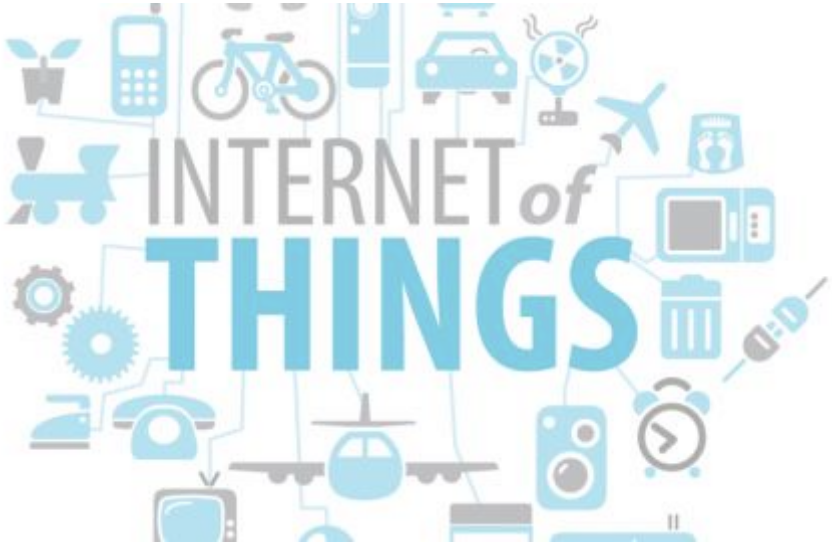
Victims:	166,349
Dollar Losses:	**$26,201,775,589**

Twenty-six billion dollar fraud scheme and growing

Source: www.ic3.gov FBI Public Service Announcement – September 10, 2019

How secure are your “IOT” devices?

- Default login credentials? (admin / password)
- Universal Plug and Play (uPNP) vulnerabilities?
- Behind a firewall with internet access blocked?



More info: FBI Public Service Announcement – October 17, 2017
https://www.ic3.gov/media/2017/171017-1.aspx

Rise of the botnet

ENTER MIRAI

- In September of 2016, a record-setting 620 Gbps DDoS (Distributed Denial of Service) attack was linked to a disturbing new trend
- Legitimate devices like IP Security Cameras were hijacked by criminal actors
- Used for conducting attacks, sending spam, and other crimes

HOW MIRAI WORKS

- Scan IP Addresses
- Attempt default logins
- Compromise devices
- Repeat steps 1-3
- Listen for commands
- Launch DDoS attacks

Source: https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Corporate account takeover

Corporate Account Takeover is a type of business identity theft where cyber criminals gain control of a business' bank account by stealing valid credentials. The criminals then initiate fraudulent wire and ACH payments to accounts under their control.

Corporate account takeover

Points of Compromise

EMAIL

Malware can be hidden within attachments or by clicking links in fake emails.

BROWSER – POP UP / DOWNLOAD PROMPT

Fraudsters are always finding creative ways to trick users into accepting malware installs.

BROWSER – DRIVE BY DOWNLOAD

Unpatched operating systems or browsers can be susceptible to vulnerabilities, allowing a 'bad' webpage to install software without the user's knowledge or consent.

USB DRIVE / NETWORK INFILTRATION

Malware can enter the workplace on a USB drive or an attacker can infiltrate a poorly secured network and execute code on vulnerable systems.

VENDOR COMPROMISE

Malware can be bundled alongside legitimate updates from a compromised vendor.

Advanced malware

RANSOMWARE

Malicious software that encrypts the victim's files and holds them hostage unless the victim pays a ransom, usually in difficult to trace bitcoin. Paying the ransom does not always result in the files being recovered and only perpetuates the scheme. Restoring from backup is often the only reliable method of recovery.

WIPER ATTACKS

Software designed to permanently destroy stored data and physically overwrite the Master Boot Record on infected hard drives rendering the operating system unbootable.

Supply chain attacks

Supply chain attacks involve malicious code inserted into legitimate software by attackers. The goal of these attacks is to gain unauthorized access to the customers of the hacked firms.

"The risks associated with a supply chain attack have never been higher, due to new types of attacks, growing awareness of the threats, and increased oversight from regulators. Meanwhile, attackers have more resources and tools at their disposal than ever before, creating a perfect storm."

MARIA KOROLOV FOR CSO ONLINE

Source: https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html

Solar winds compromise

HIGHLY SOPHISTICATED ATTACKER(S)

- Multiple sources point towards the threat actor being one or more nation-states
- Attack code appears to be the work of a dedicated team of experts

ENORMOUS SCOPE OF BREACH

- Victim customers of Solar Winds include multiple departments of the U.S. Government as well as both public and private organizations across the globe
- Solar Winds disclosed via SEC filing as many as 18,000 customers may be affected

POST INFECTION ACTIONS

- Targeted entities saw the attackers act quickly to expand their network access
- Attackers took control of victim's IT infrastructure to ensure they retained access even after the Solar Winds product was removed
- Issued access tokens allowing further privileges such as reading and sending email

ATTACK TIMELINE

- Solar Winds breached October, 2019
- First modified file delivered to customers March, 2020
- Attacker infrastructure taken offline December, 2020

Source: https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

Data breaches

EQUIFAX – 145.5 MILLION RECORDS

- Includes SSN, drivers licenses, other data
- Breached May 2017
- Publicly announced Sept. 2017
- Revised Oct. 2017

YAHOO – ALL EMAIL ACCOUNT HOLDERS

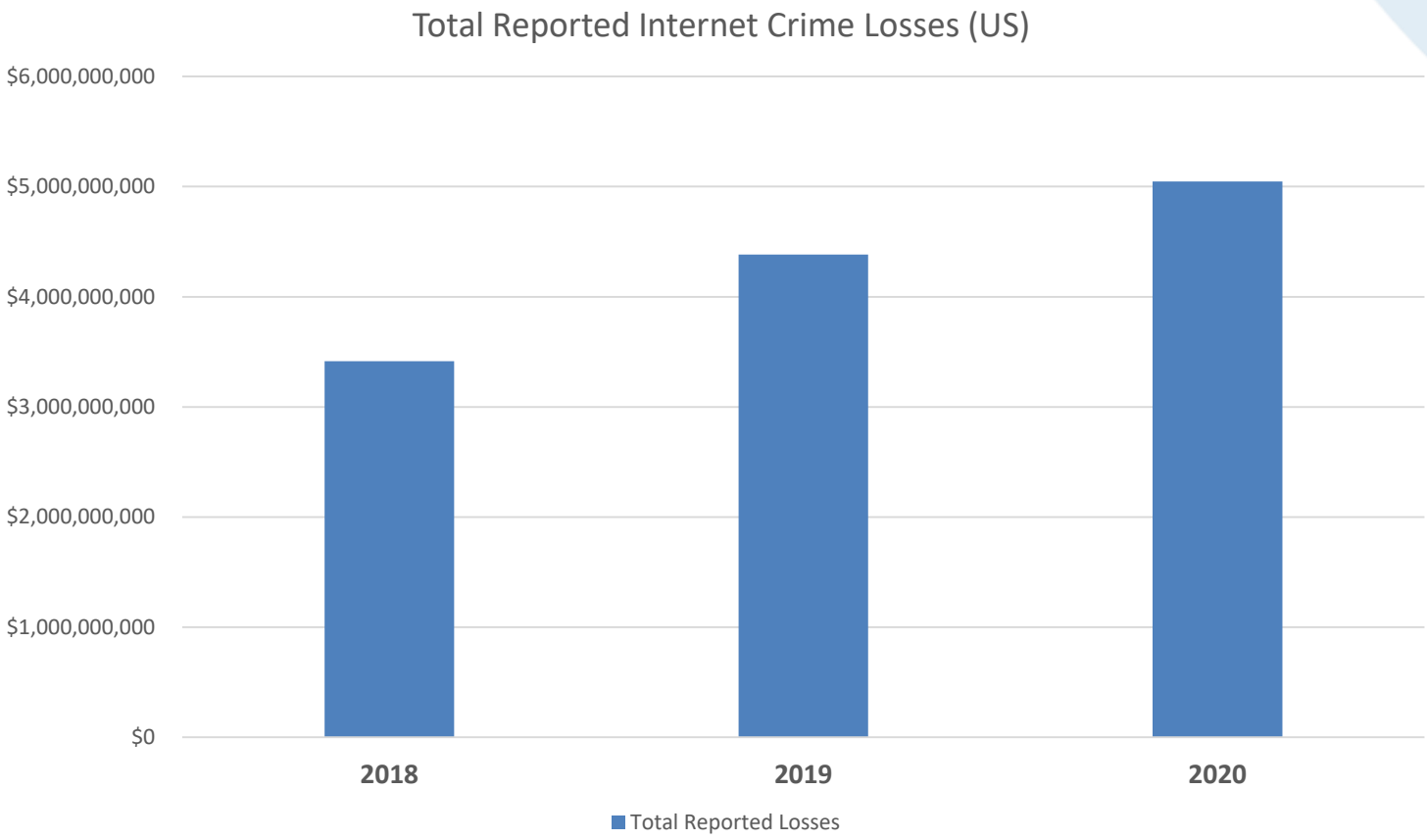
- Includes login, password, secret questions
- 3 billion accounts affected
- Breached Aug. 2013
- Publicly announced Dec. 2016
- Revised Oct. 2017

Sources:

https://investor.equifax.com/news-and-events/press-releases/2017/10-02-2017-213238821

https://www.verizonmedia.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/

Cyber crime on the rise



Source:

https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Passwords

WEAK PASSWORDS

- Dictionary words
- Easily guessed
- Short length

STRONG PASSWORDS

- Indecipherable meaning
- 12 or more characters
- Use upper and lower case
- Use numbers and symbols

1. 123456
2. 123456789
3. picture1
4. password
5. 12345678
6. 111111
7. 123123
8. 12345
9. 1234567890
10. senha
11. 1234567
12. qwerty
13. abc123
14. Million2
15. 000000
16. 1234
17. iloveyou
18. aaron431
19. password1
20. qqww1122

Source: NordPass's worst passwords of 2020

Prevention

Personal

CHECK PAYMENTS AGAINST SOURCE DOCUMENT

- Don’t trust email for payments, especially if time pressure is being applied

MONITOR CREDIT REPORT REGULARLY

- www.annualcreditreport.com up to 3x per year (1 per credit bureau)
- Consider a credit monitoring service or freezing your credit if a victim

USE STRONG, UNIQUE PASSWORDS

- Implement multi-factor authentication (tokens) if available

PATCH COMPUTERS AND PROGRAMS REGULARLY

- If it is installed, patch it. Even if you don’t use it. Don’t ignore that Windows update!

MONITOR ACCOUNT STATEMENTS AND CARD ACTIVITY

- Reg. E protects consumers up to 60 days after the statement fraud appears on
- The sooner you discover and stop the fraud, the better

Prevention

Business

MONITOR ACCOUNTS DAILY

- 24 hours or less to detect and respond to fraud

USE A FIREWALL AND INTRUSION PREVENTION SYSTEM

- Don’t use default or generic passwords anywhere
- Ensure internal devices are not accessible from the internet

ACH AND WIRE OPERATORS SHOULD BE IN DUAL CONTROL

- One person submits items, another person approves them
- Verify change requests by following established procedures

PROTECT YOUR WEAKEST LINK

- Train employees to recognize cyber threats and be aware at all times
- Prevent phishing attacks with email filters and continuous training

DO MORE THAN THE MINIMUM

- Establish an ACH debit filtering solution such as ACH Fraud Prevention
- Don’t forget about checks! Positive Pay can prevent taking a loss

Best practices

1. Be suspicious of requests for secrecy or pressure to act.
2. Confirm payment instruction changes out of band.
3. Educate employees to increase awareness.
4. Use separation of duties as a control to prevent fraud.
5. Limit physical and logical access to your PCs and devices.
6. Shield your networks from unauthorized access.
7. Use rules to flag or block potentially fraudulent emails.
8. Regularly patch all systems and programs.
9. Backup important data and test backups regularly.
10. Have a disaster plan to ensure business operations.

Ask yourself one question

How much are you willing to lose?

Thank You

Mike Mason
Product Support Manager
MMason@FNBAlaska.com
777-3649