IMPACT 2022

CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

Navigating the Ever-Changing Threat Landscape

National Credit Union ISAO

Presented by Brian Hinze
VP, Member Services & Operations

Session Overview

- Introduction
  - Who is NCU-ISAO?
  - How this presentation will work
- Recent Cybercrime Statistics
- Global Threats
- Financial Services & Credit Unions
  - Common Threats
  - New Trends & Other Threats
- Common Best Practices to Apply

A Quick History of the NCU-ISAO…

Enabled by the **CISA Act of 2015**, the NCU-ISAO began in concept with a credit union specific call to help lead credit unions to **cyber resilience**…

- A collaboration of Credit Unions, CUSOs, and Leagues
- Help navigate the flooded waters of threat intelligence and alerts
- Focus on credit union-specific issues around operations, risk, compliance through information sharing and collaboration

How This Presentation Will Work

- We'll working our way through the Threat Universe
  - Top-down into more CU-specific and novel threats
  - Reviewing applicability and some best practices for each

Recent Cybercrime And Fraud Overview

What do Threat Actors want and how do they get it?

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

IBM 2021 Cost of a Data Breach Report

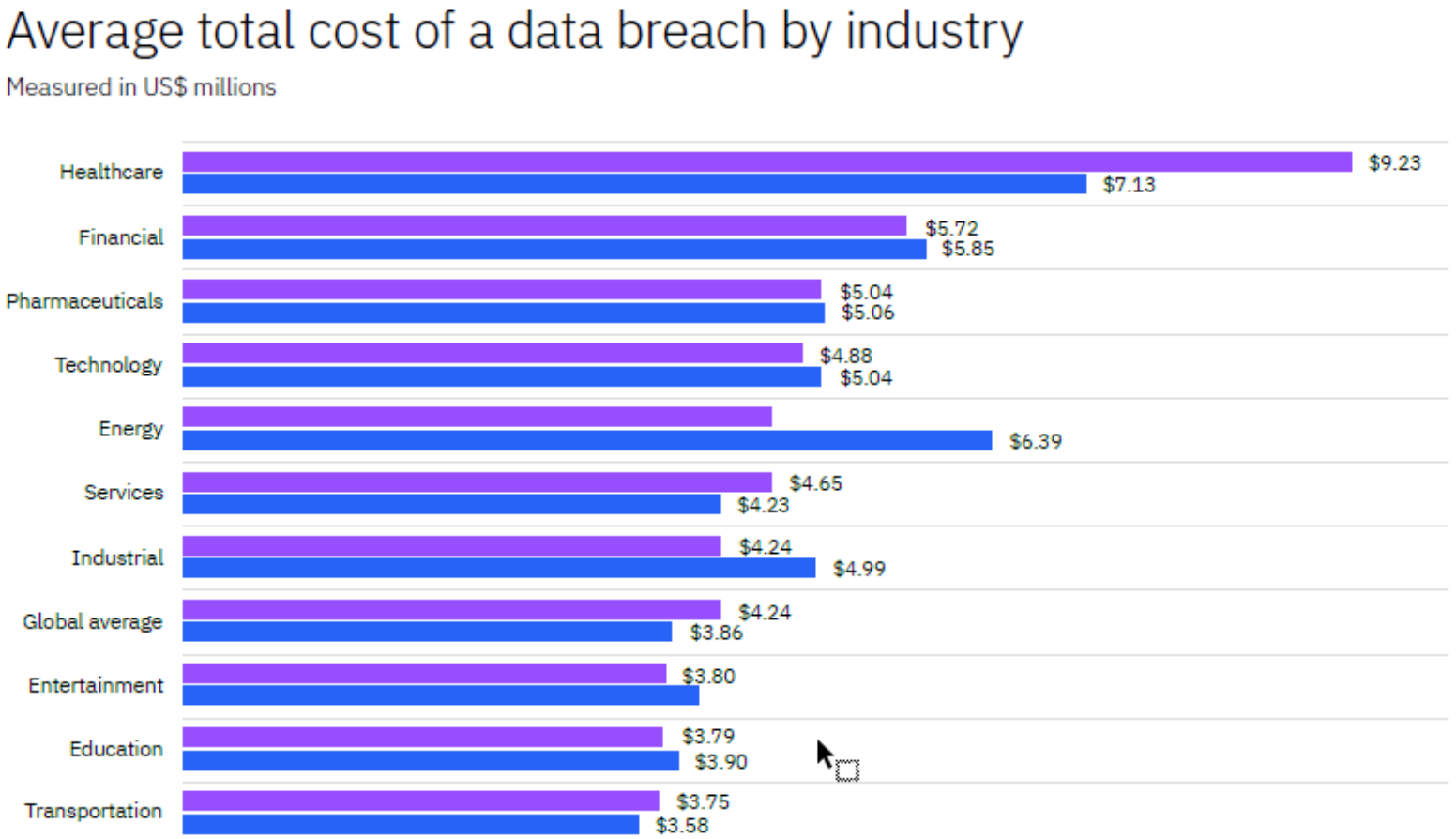
IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

Key finding

$4.24m

Global average total cost of a data breach

- $5.72m in Financial Services
- United States Overall Cost is $9.05m

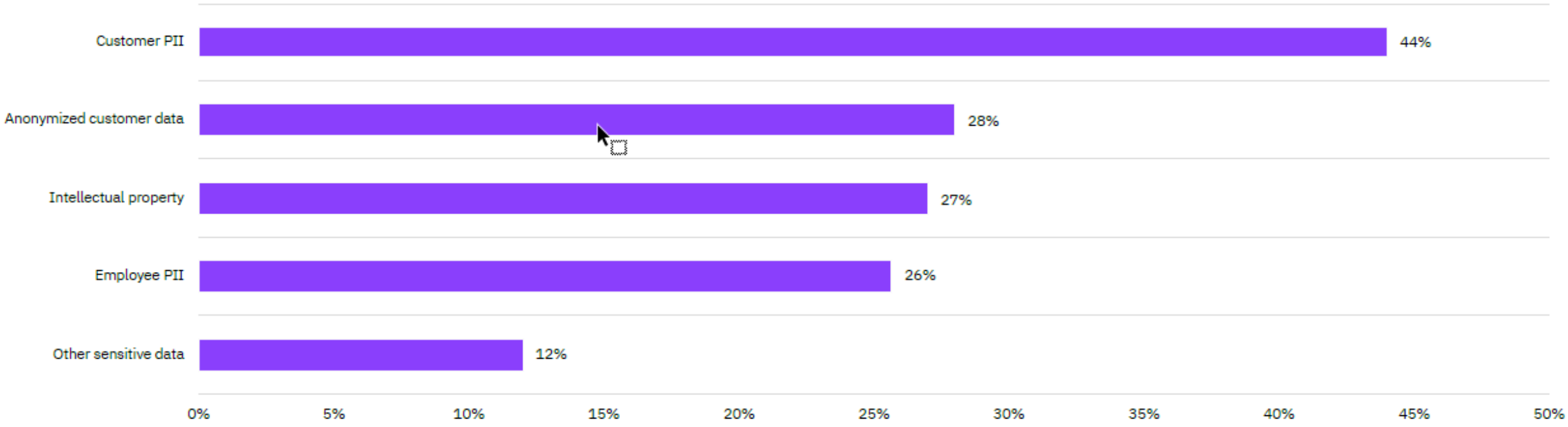


IBM 2021 Cost of a Data Breach Report

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

Types of records compromised

Percentage of breaches involving data in each category

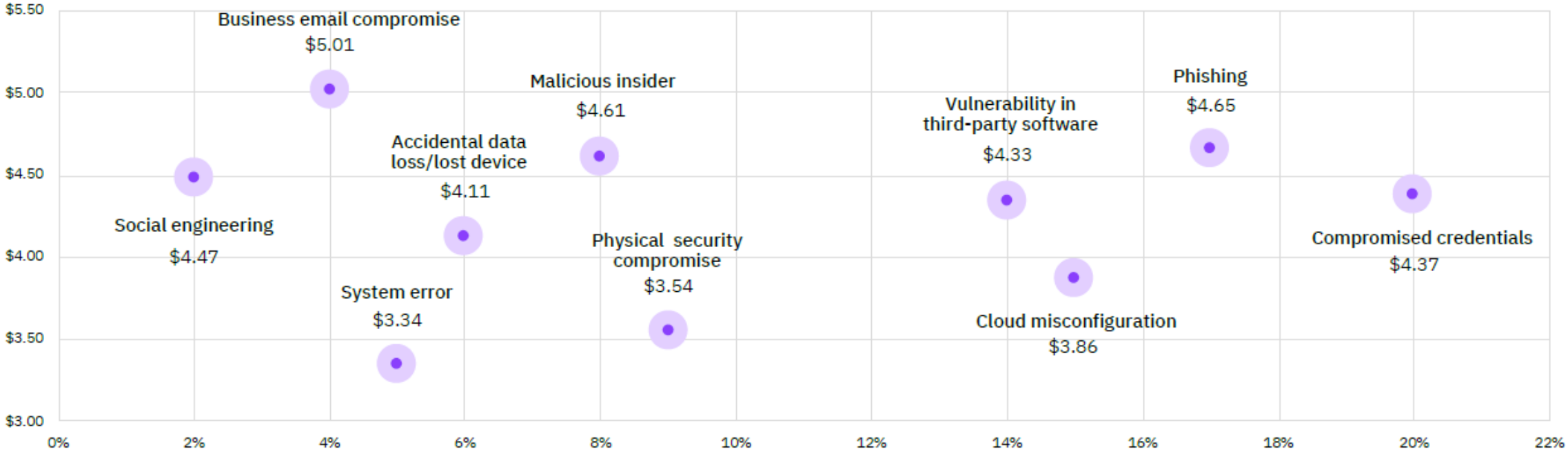


IBM 2021 Cost of a Data Breach Report

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

Average total cost and frequency of data breaches by initial attack vector

Measured in US$ millions



Verizon 2021 Data Breach Investigations Report

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

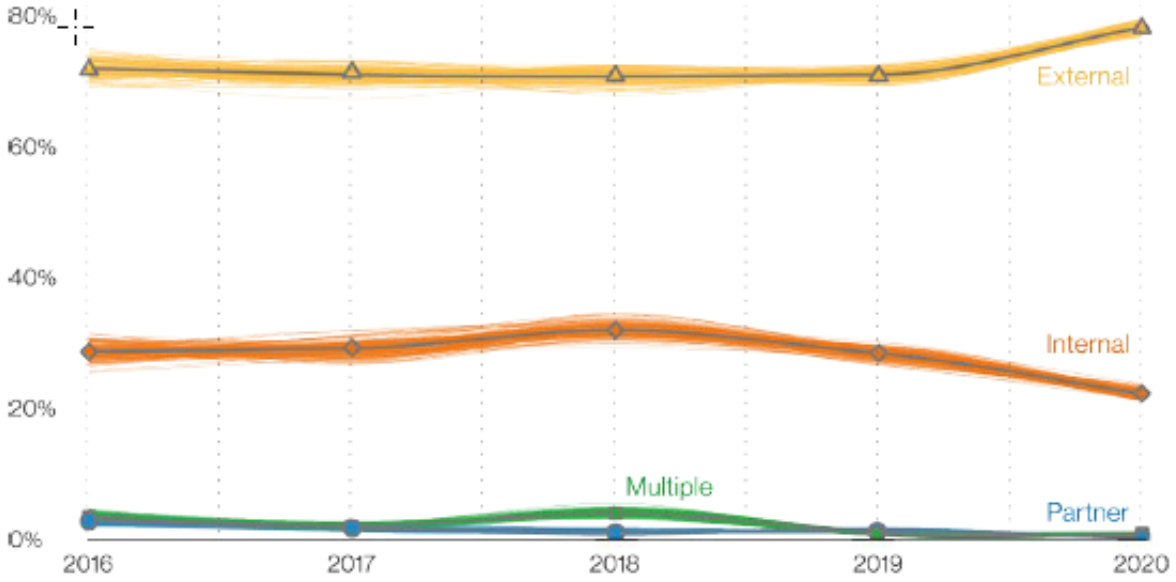


Figure 14. Threat actor over time in breaches

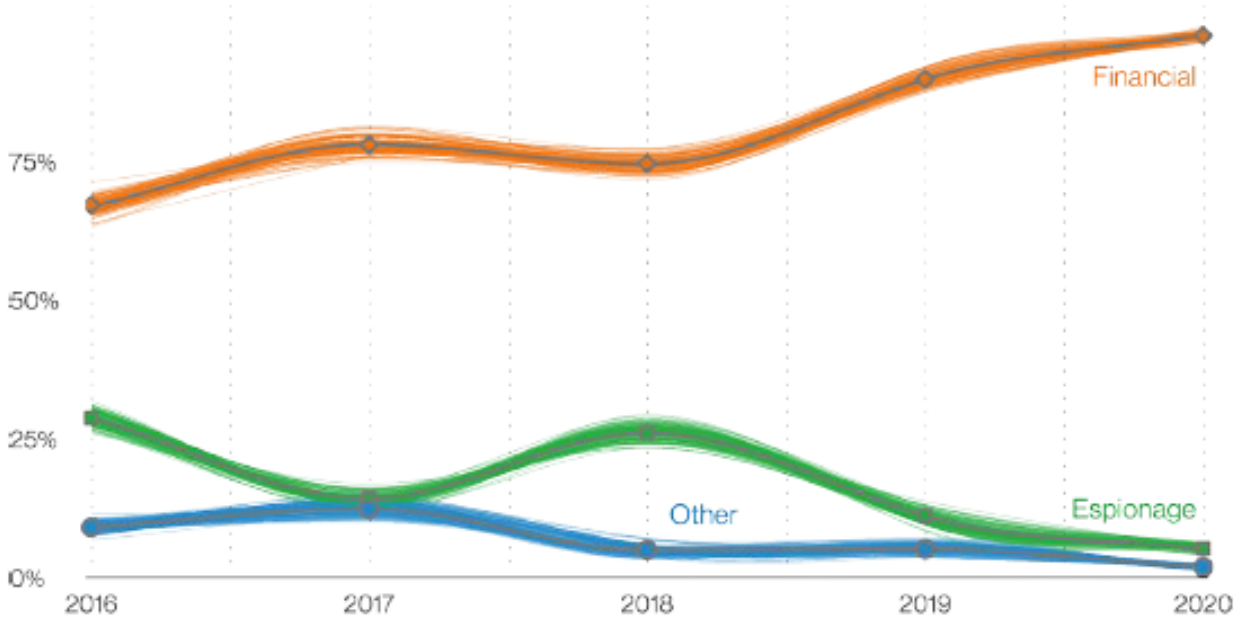


Figure 15. Top threat actor motive over time in breaches

Global Threats

The cyber threats all industries are facing today

Nation States

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

Sophisticated, advanced, nation-backed cyber threats commonly focused on:

- Intelligence gathering and espionage
  - Compromising governments and militaries
  - Compromising critical and physical infrastructure entities
- Stealing trade secrets and intellectual property
- Disinformation and swaying public opinion
- Monetary gain

Common nation-state adversaries:

- Russia
- China
- Iran
- North Korea

Primary threats to banks and credit unions:

- Software/service supply chain and other sophisticated, difficult to detect attacks
- Business disruption targets:
  - Indirectly: compromise or loss of connectivity to networks and/or partners
  - Directly: DDoS or other attacks intending to disrupt US financial systems, or theft of financial information on clients/members

Defending against nation-state attacks:

- Keep software up-to-date
- Effective backup of critical data
- Being prepared with good incident response planning and business continuity
- Taking quick action if a possible intrusion has been observed

https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/
https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf

Nation States (cont…)

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

Business continuity and global infrastructure attacks during conflict - Russia/Ukraine conflict had/has a significant cyber angle to it:

- Russian GRU attacks on Ukrainian Gov't and Financial Services targets
- Ukraine hired an army of 'hackers' to support its efforts
- Allied countries for both saw increased cyber activity
- Other nation states ramp up activity and disruptive efforts

- **Business disruption targets gleaned from this conflict:**
  - Corporate attacks – see previous slide
  - Disrupt a country's ability to do business and operate normally
    - Financial
    - Physical/Communication

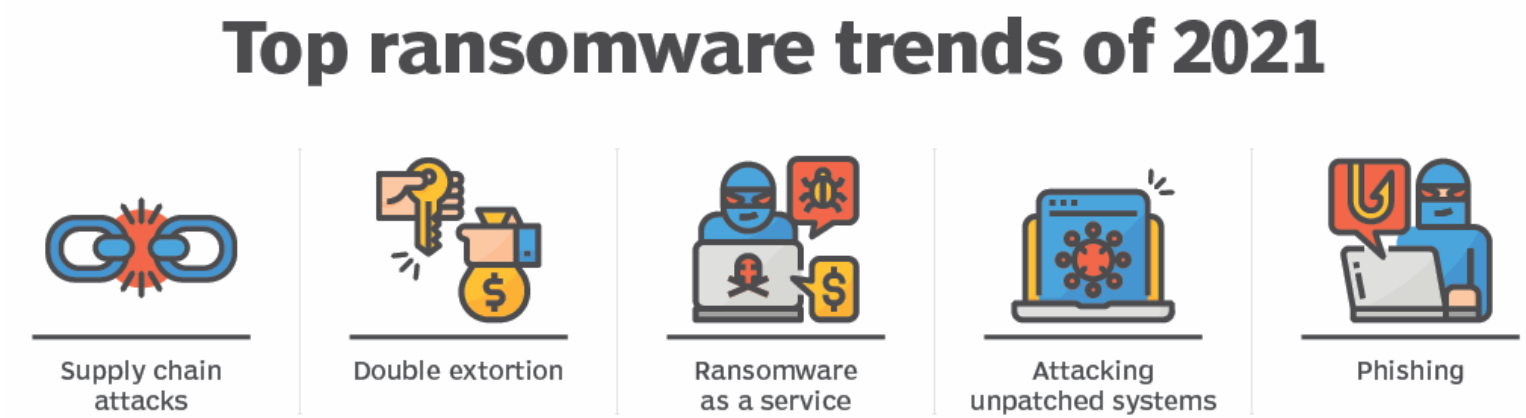
Defending against nation-state attacks – business disruption and global conflict:

- In addition to strategies above, be prepared:
  - Assess exposure and visible attack surface – what is exposed to the internet?
  - Watch B2B connections
  - Stay informed through partners, open sources, information sharing orgs
  - Educate employees on risks and follow known best practices already discussed

https://www.darkreading.com/threat-intelligence/7-steps-to-take-right-now-to-prepare-for-cyberattacks-by-russia

Ransomware

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM



According to Flashpoint (TLP:GREEN), there were 54 organized 'Ransomers' from Feb. '21 to Feb '22, accounting for nearly 3,100 infections.

- Conti and Lockbit were the most successful/active in this time frame.
- Approx. 1,100 of these were against US companies, but only 3% across the Financial Services industry

Threats to banks and credit unions:

- Often starts with an open door from a phishing email, or scanning & reconnaissance activity by the threat actors targeting an FI
  - Initial Access Brokers (IABs) often compromise a system then sell the access to other firms

Defending against ransomware:

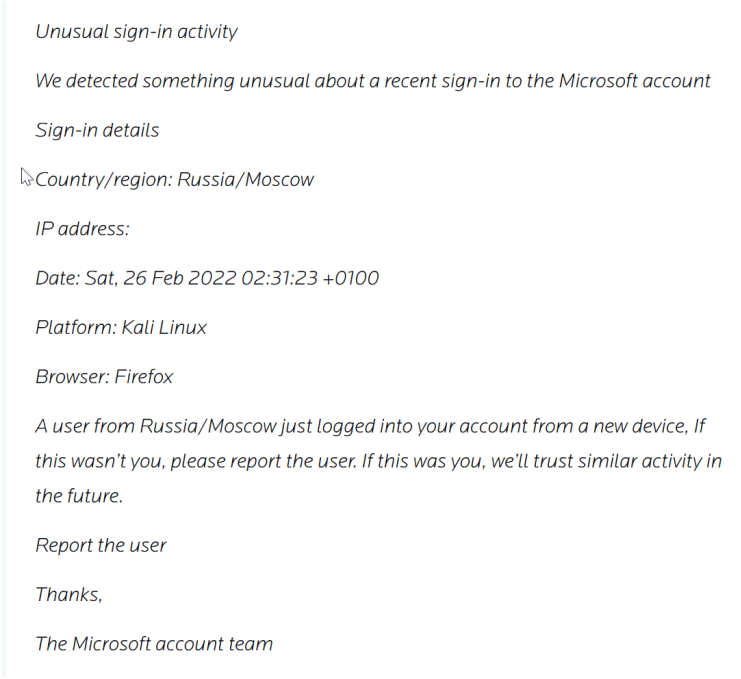
- Keep all software up-to-date
- Effective backup of critical data
- Employee phishing training & awareness

Image Credit: https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts
Ransomware data: https://flashpoint-intel.com (closed source resource)

Malicious Spam Email (Malspam)

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

- According to Kaspersky, almost half of all emails in 2021 were spam
  - Almost 25% of this was Russian in origin, with the second largest percentage coming from Germany (15%)
  - Aside from easy-to-spot social engineering attempts (charity scams, financial scams, etc.), they will often try to use universal themes to deliver 'branded' malware like Emotet, Dridex, keyloggers, ransomware, trojans and more
    - Password reset
    - Copyright violation
    - Secure file shared
    - Brand abuse
    - COVID-19



Unusual sign-in activity

We detected something unusual about a recent sign-in to the Microsoft account

Sign-in details

Country/region: Russia/Moscow

IP address:

Date: Sat, 26 Feb 2022 02:31:23 +0100

Platform: Kali Linux

Browser: Firefox

A user from Russia/Moscow just logged into your account from a new device, If this wasn't you, please report the user. If this was you, we'll trust similar activity in the future.

Report the user

Thanks,

The Microsoft account team

Threats to banks and credit unions:

- Fortunately, a large percentage of spam is caught by email appliances, filters and marked junk
- Those that are successful though, may compromise data, accidental systems access, lead to botnets, backdoors and more

Defending against Malspam:

- Deploy email security software and/or appliances
- Employee phishing training & awareness is number
  - Look for odd file attachments and file types
  - Look for out of nowhere, unknown senders on strange topics

https://securelist.com/spam-and-phishing-in-2021/105713/
https://blog.malwarebytes.com/scams/2022/03/unusual-sign-in-activity-mail-goes-phishing-for-microsoft-account-holders/

Insider Threats

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

2022 Ponemon Cost of Insider Threats Global Report:

- The cost of credential theft to organizations increased 65% from $2.79 million in 2020 to $4.6 million at present.
- The time to contain an insider threat incident increased from 77 days to 85 days, leading organizations to spend the most on containment.
- Incidents that took more than 90 days to contain cost organizations an average of $17.19 million on an annualized basis.
- *Risk increased with remote work*

- **Two main types of insiders:**
  - Malicious
  - Accidental/unwitting

- **Two examples:**
  - Disgruntled CU employee deleted 21GB of data
  - (Even impacts criminals) Conti gang member leaked damaging information forcing them to reorganize

https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats
https://www.cisa.gov/insider-threat-mitigation

Threats to banks and credit unions:

- Loss of sensitive information, public leaks, or other
- Complete system compromise
- Loss of reputation

Mitigating Insider Threats:

- Employee training & awareness
- Knowing who has privileged access
- Know early indicators
- Manage systems access carefully during M&A
- Deploy policies, frameworks, tools
  - Data Loss Prevention
  - Zero Trust
  - Next-gen tools
- Develop a program – CISA has a guide that will walk you through it:
  - Insider Threat Mitigation Guide & Assessments (see reference link)

Other Global Threats…

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

Accellion FTA, SolarWinds, Kaseya, Kronos and others are examples of high profile security challenges in today's connected world, where companies find themselves impacted directly by breaches at other companies.

Furthermore, zero-day vulnerabilities like Microsoft Exchange ProxyLogon/Proxy Shell and Log4j, a where there is no immediate fix, put credit unions in a difficult position to understand a broad range of attack surfaces.

Securing remote work has proven difficult for many organizations, as can reduce security in some respects and make it more difficult to secure sensitive data and reduce insider risk.

Risks to Banks and Credit Unions

- Potentially caught off-guard by a third-party or fourth-party breach or attack
- Downstream attacks like those we've already covered, such as ransomware or business disruption
- Insider Risk
- Others

Best practices for these other global threats:

- Understand where vendors and partners have access is in your network and what the exposure is
- Stay informed on the latest threats and vulnerabilities
    - Track vulnerable "zero-days" and apply mitigations recommended by the software provider and apply patches immediately when they become available
- Other

Financial Services & Credit Unions

Important to Know Threats to CUs, and Trends We're Seeing

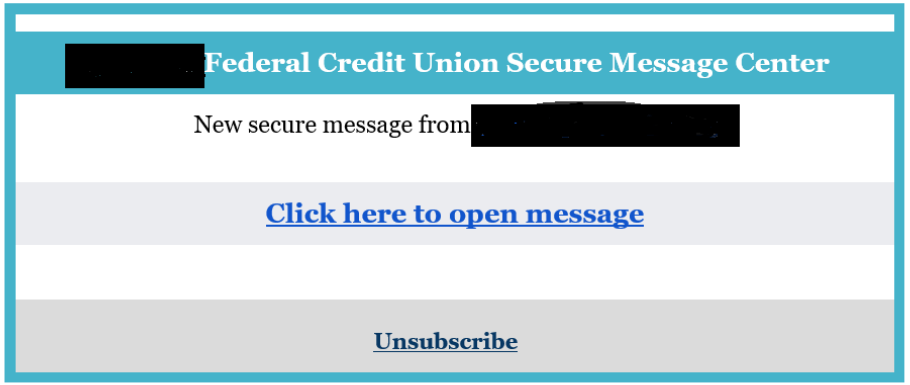
IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

Phishing Attacks

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

In a previous section, we discussed malware distributed by spam, but here are some a few notable phishing tactics observed by CUs:

- **C-suite / Business Email Compromise**
  - Often, information is collected or scraped via public or semi-public sources like LinkedIn or Facebook
  - Non-compromised accounts are spoofed
  - Attempt to get information or money leveraging a person's status
- **Compromised sender accounts**
  - Very effective phishing campaign to steal MS credentials
  - Looks like a common, branded (or generic) secure message
  - Comes from other compromised, legitimate senders
  - Steals all victim contacts and redistributes it
  - Stolen credentials of privileged users pose a huge risk
- **CU spoofed password resets**
  - Pretend to be IT admin emails, but really grabbing credentials



Risks to Banks and Credit Unions

- Many – arguably the biggest risk to CUs, but certainly the biggest threat surface, as all employees with email are at risk

Best practices for mitigating phishing attacks:

- Employee education on the latest TTPs
- Filter out malspam with next generation email tools
- Information sharing to tell other CUs about the new tactics your CU is seeing

Source: Closed intelligence via NCU-ISAO shared information

Back to the Verizon 2021 DBIR…

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

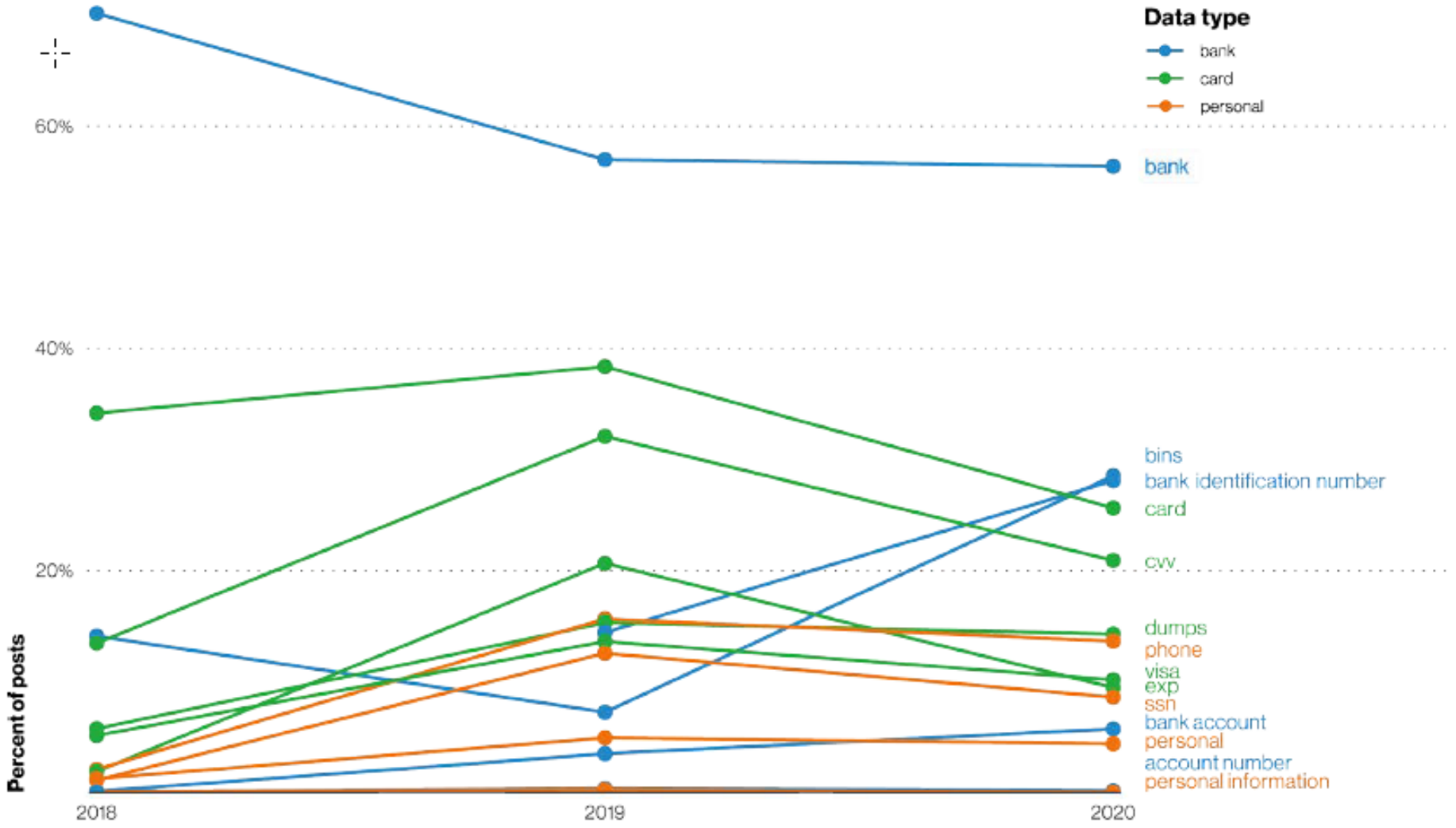
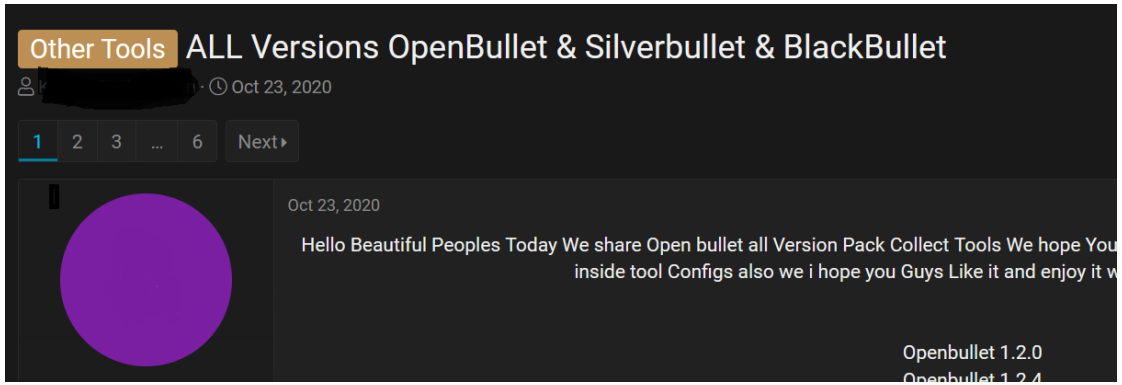


Figure 17. Terms over time in criminal forums and marketplaces

Member Account Takeover & Credential Stuffing

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

Widely available pen-testing tools or other custom software are commonly abused to target online banking login web pages. Attackers use widely available lists that combine user logins and their compromised passwords (combolists). Together, they are used to attack banking sites, hoping for passwords to be reused and no MFA enabled. These hacked accounts can sell for $100 and up, depending on how much money is in their accounts.



Risks to Banks and Credit Unions

- Compromised accounts cost FI's money, reputation, and the member's accounts get drained
- Stolen PII, CC information facilitate mobile deposits fraud, exfiltrate funds, and more…

Best practices for mitigating credential-stuffing type attacks:

- IP Rate limiting
- Captchas
- Force or encourage multi-factor authentication (MFA)
- Have credential stuffing plans in place with hosting providers

Source: OSINT, closed intelligence and via NCU-ISAO shared information

Plastic Card Fraud

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

2021 was a tough year for plastic card fraud, as there were multiple dumps, Telegram provided additional accessibility, and e-skimming continues to evolve.

2021 Data – Includes Duplicates*:
- As many as 500M U.S. cards in 2021 (closed source intel)
- 295M card not present
- Millions also seen in card checking services (bots used to check for validity)

2022 Data – Includes Duplicates:
- Already 11M U.S. cards (financial services) observed on fraud channels between Jan-Feb 2022 (closed source intel)

Interesting fact: cards get stolen, then sold, resold, checked, and so on at a rate of 7-20 times over. Even after being canceled by the FI.

Common places where cards are transacted on:

- Premium and pay-to-play shops on the deep/dark web
- Telegram channels
- Open web
- Paste sites
- Bots, checkers

*There are far too many fraud channels, sources, shops and repeat card fraud sightings to provide accurate data. Source: Closed intelligence via NCU-ISAO partner resources & datasets

Plastic Card Fraud

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

How the stolen cards are obtained:

- E-skimming (Magecart attacks)
- Fraudulent online purchase or donation scams
- Physical theft and skimming
- Social engineering
- Synthetic identities
- Generated using algorithms
- Hacking/Account takeover
- Bad consumer hygiene

Risks to Banks and Credit Unions

- Monetary loss
- Reputational risk with individual consumers/members
- Overburdening Fraud departments or issuers
- Other

Best practices for mitigating card fraud:

- Employ the latest detection and mitigation best practices
- Leveraging one or many real-time monitoring services
  - Processor-level
  - Dark Web services
    - Card fraud mitigation
- Member education on fraud tactics, safe browsing and online shopping, not sharing private information
  - Using chip cards
  - Checking for skimmers
  - Not sharing sensitive information
  - Limiting amount in checking accounts
  - Other

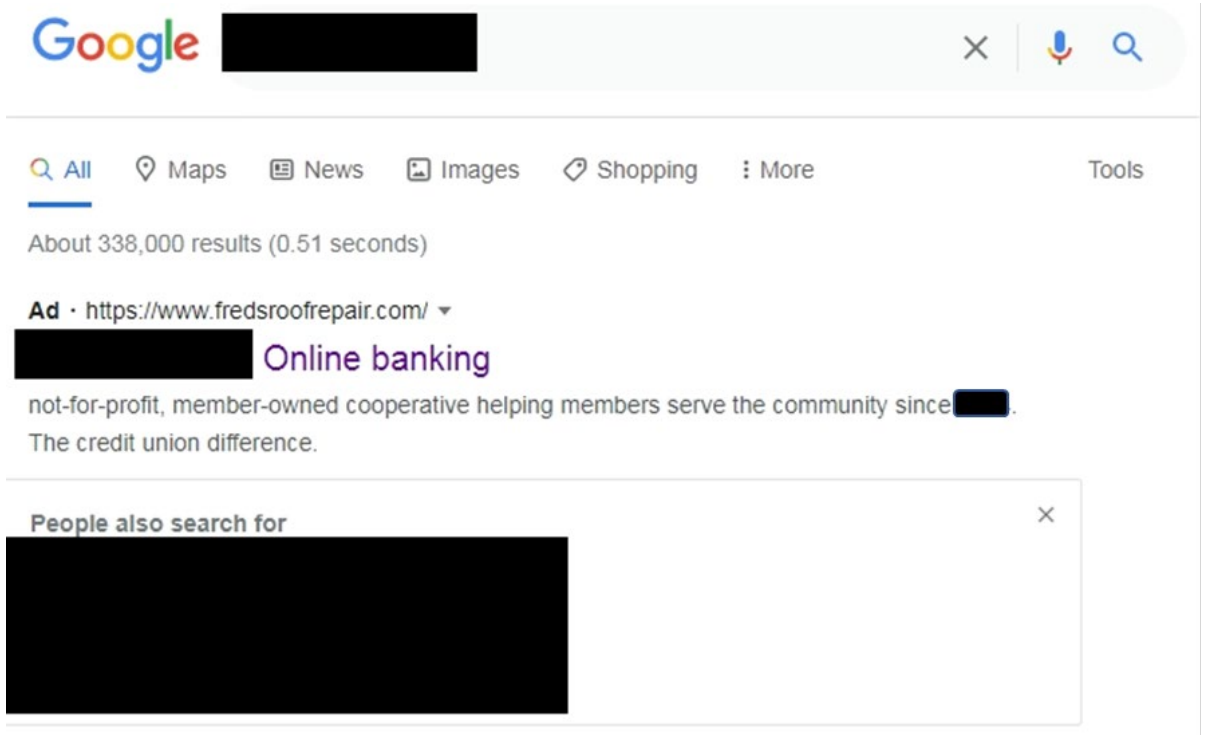
*There are far too many fraud channels, sources, shops and repeat card fraud sightings to provide accurate data
Source: Closed intelligence via NCU-ISAO partner resources & datasets
Best practice source: https://www.desertfinancial.com/news-and-knowledge/protect-your-money

Other Trends and Threats Seen by CUs

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

Novel and Trending Attacks:

- SEO Poisoning / Google Adwords Targeting
  - Trick Google users to going to a fake login site
  - Steals login credentials
- SMS & Higher Authority Gift-card scams
  - Tricking employees to buying gift cards
- MFA Scams – Member attacks used for session takeover and Fintech app linking (like Zelle)
  - No CU chargeback rights under Reg E
- Fraudulent new member accounts
  - Mass opening of online accounts
  - Synthetic IDs
  - Used for fake mobile deposits, etc.



Source: Closed intelligence via NCU-ISAO shared information

Common Lessons, Themes & Takeaways

Using Knowledge of Past Event to Protect in the Future

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

Common Themes and Best Practice Review

IMPACT 2022
CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

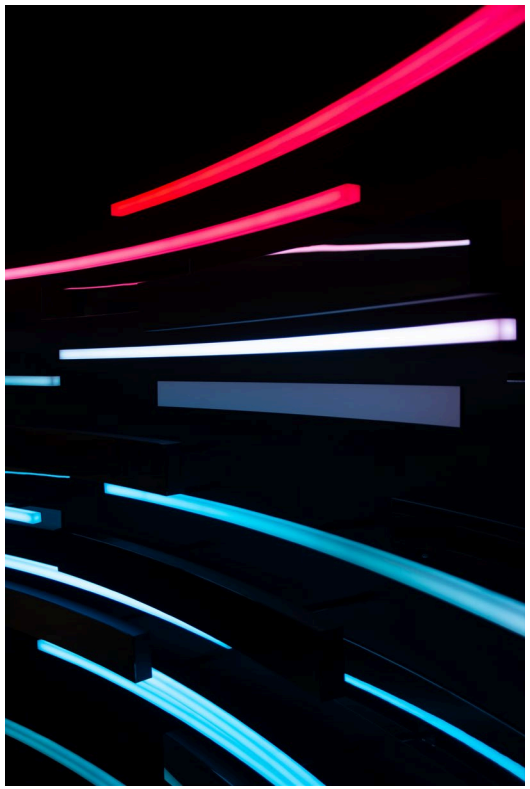
What can you do to reduce your risk as a credit union (the Big 3):

1. Require complex passwords and do not allow reuse - better yet, deploy a password manager

2. Use multi-factor authentication whenever possible, and certainly wherever sensitive data access is located

**Educate CU members on the benefits of both of these above to help secure their accounts – great resources are available at staysafeonline.org*

3. Keep software up-to-date – if you have a legitimate reason patching cannot occur, understand and monitor threats related to these vulnerabilities



BONUS: Share information! We are all stronger when we know the latest tactics and threats. If you see something, say something.

Source: Closed intelligence via NCU-ISAO shared information

THANK YOU!

CORNERSTONE ANNUAL MEETING & COUNCIL FORUM

IMPACT 2022

Questions? I'm happy to help:

Brian Hinze
VP, Member Services & Operations
NCU-ISAO
Brian.hinze@ncuisao.org

Learn more about us at: https://ncuisao.org/

Attend our annual conference – CU Intersect in July (Houston, TX): https://cuintersect.com

Save $150 with code CORNERSTONE2022

CORNERSTONE ANNUAL MEETING & COUNCIL FORUM
IMPACT 2022

1. https://www.verizon.com/business/resources/reports/dbir/
2. https://www.ibm.com/security/data-breach
3. https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2021/10/Sample-Nation-State-Actors-scaled.jpg
4. https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/
5. https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf
6. https://www.darkreading.com/threat-intelligence/7-steps-to-take-right-now-to-prepare-for-cyberattacks-by-russia
7. https://securelist.com/spam-and-phishing-in-2021/105713/
8. https://blog.malwarebytes.com/scams/2022/03/unusual-sign-in-activity-mail-goes-phishing-for-microsoft-account-holders/
9. https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats
10. https://www.cisa.gov/insider-threat-mitigation