FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 21 October 2024 | Vol. 253

We encourage you to share this report with other senior executives or incorporate it into your regular reporting processes.

This Week's Threats

Fraud Campaigns

- Account takeover
- Call center
- CEO impersonation
- Customer validation
- Employee impersonation
- New account fraud
- Online account
- Withdrawal and enrollment

Threats, Malware, Cyber Campaigns, and Adversaries

- Astaroth
- AsyncRAT
- Badger (aka BOLDBADGER) Malware
- ClickFix / ClearFake
- Credential Pharming
- Credential Validation
- Formbook
- Grandoreiro
- JsOutProx RAT
- Latrodectus
- LandUpdate808
- NetSupport RAT
- Payroll Diversion
- Salt Typhoon
- SocGholish
- StrelaStealer
- UnitedFullz Telegram Bot
- Ursa
- VenomRAT
- Xloader

System Vulnerabilities

Cisco, Cygwin, Debian, Dell, Fortinet, GNU C Library, Google, IBM, Ivanti, Juniper, Lenovo, Linux, Magento, Mozilla, NVIDIA Quadro, Oracle, Palo Alto, Red Hat, Samsung, Spring Security, Ubuntu, VMware.

Themed Phishing and Smishing Campaigns

Please see the Phishing Daily Digest for all activities. Use keywords for AV blacklists.

Subject Keywords: ***Action Required***: Verify Your Registered, An Urgent Review Requires Your Attention Immediately, ATTENTION REQUIRED, DocuSign, ICANN, !ncoming V-Message, Intuit, Manipulated invoice, Message Payment Confirmation, Pending Rev!ew, Money On The Way!!, Okta, Outstanding Invoice, Remittance Advice, Renouvellement Services, Request for offer, See attached CSV file, SharePoint, Statement S29308 Outstanding, Suspicious Activity Detected On Your Account, and Unrecognized Network Access.

NEWS AND RISK INFORMATION

Analyzing a multi-stage malware attack targeting digital marketing professionals. Spam emails containing phishing attachments primarily target digital marketing, e-commerce, and performance marketing professionals, especially those involved in Meta advertising in the US, and facilitate data exfiltration and, potentially, deployment of additional malware. (The Cyber Express)

Early cascade injection technique enables Windows process creation and stealthy injection. Researcher Guido Miggelenbrink from Outflank has introduced a new process injection method called Early Cascade Injection. This technique adds sophistication to evading Endpoint Detection and Response (EDR) systems, challenging even top-tier EDRs. (outflank)

F5 BIG-IP vulnerability leads to access control bypass, PoC available. A critical vulnerability (CVE-2024-45844) in F5 BIG-IP allows authenticated attackers to bypass access control, potentially compromising systems. The flaw exists in the BIG-IP monitor functionality. (Cybersecurity News)

Fortinet releases patches for undisclosed critical FortiManager vulnerability. Fortinet has issued critical security updates for FortiManager to address a vulnerability exploited by Chinese threat actors. The company privately informed select customers of the issue and provided temporary mitigation advice. (Help Net Security)

From Windows to Linux to ESXi: The Cicada3301 ransomware hits them all. The Cicada3301 ransomware group, discovered in June 2024, has targeted 30 organizations in critical sectors in the US and UK. Operating an advanced affiliate program, Cicada3301 recruits penetration testers and brokers to carry out attacks. (Security Online)

GHOSTPULSE employs new pixel-level deception to hide in PNG files. Elastic Security Labs has discovered a significant development in the GHOSTPULSE malware family, which now hides its payload within the pixel structure of PNG files to evade detection. (Elastic)

Iranian hackers conduct brute force and password spraying to compromise critical infrastructure organizations. A joint US, Canadian, and Australian cybersecurity advisory warned of Iranian cyber actors using brute force and other methods to compromise organizations, particularly in critical sectors such as healthcare, government, IT, engineering, and energy. (US-CERT)

macOS vulnerability could expose user data, Microsoft warns. Microsoft has found a macOS vulnerability named "HM Surf" that allows attackers to bypass the operating system's Transparency, Consent, and Control (TCC) technology to access users' browsing history, camera, microphone, and location. (Infosecurity Magazine)

New York detective indicted for darknet card data buys. A Federal Bureau of Investigations (FBI) probe into shuttered cybercrime site Genesis Market has led to the indictment of Terrance Ciszek, a now-suspended police detective in Buffalo, New York, who's been accused of buying stolen payment card data and recording a video showing fraudsters how to use it anonymously. (Data Breach Today)

North Korea's fake IT worker scheme now extorts employers. Demanding ransoms for stolen data is the latest extortion tactic in a larger operation involving stolen or fake identities that place individuals within companies across North America, Europe, and Australia. (The Record)

Unmasking Lumma Stealer: analyzing deceptive tactics with fake CAPTCHA. The malware's execution relies on legitimate tools like PowerShell and mshta.exe. Once the fake CAPTCHA is clicked,

a Base64-encoded PowerShell script is copied to the clipboard, triggering the download of a stager file. (Qualys)

THREATS OF THE WEEK

Monetizing compromised financial information highlights this week's risks

Data to Dollars

Summary

Have you ever wondered how counterfeit checks are fabricated? Read this for a high-level overview of how it's done. For more detailed discussions, talk with your institution's fraud team.

Getting Personal Information

According to a 30 January 2024 report from Ravelin, a 12TB "database of "fullz" – a fraudster term for sets of personally identifiable information (PII) – was discovered by cyber threat researcher Bob Diachenko. The report also the database is "estimated to be the largest set of breached credentials ever discovered, at 26 billion records … an aggregate record of more than 3,800 data leaks."

For fraudsters, this is a huge canvas to work from, but they incorporate other techniques to counterfeit checks as well.

The following, generated by Google AI, lists common tactics, techniques, and procedures (TTPs):

Social media: Fraudsters can look at your social media posts and photos to find identifying information.
Public WI-FI: Fraudsters can get personal information from your phone when you use public Wi-Fi.
Phishing: Fraudsters can use fraudulent emails, texts, or phone calls to get information from you.
Online quizzes and surveys: Fraudsters can ask you for personal information in online quizzes and surveys.
The account holder: Fraudsters pay the account holder for a copy of their demand deposit account.
Bank statements and documents: Fraudsters can go through your trash to retrieve bank statements or tax documents.
Companies: Companies may sell your email address or phone number.
Photo IDs: Fraudsters can alter photographic identification, such as a driver's license, to create a new identity.
Skimming: Fraudsters can steal information as a debit or credit card is swiped.
Dark web: Fraudsters can purchase information on the dark web.

Fabricating Counterfeit Checks

With affordable software, hardware, color copiers, magnetic ink, and high-quality printers, fraudsters can create reasonable to nearly undetectable counterfeit checks.

Figure 1 is an example of a legitimate check specimen. Note the account holder's name, routing number, account number, and check number.

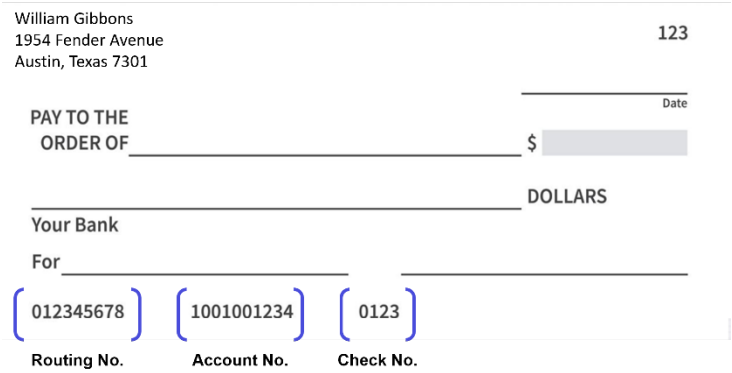


Figure 1. Legitimate Check Example

In Figure 2, a counterfeit check specimen was created using PowerPoint. You can see how easy it would be to change information just by copying and pasting from the original, then changing the name, contact information, routing number, account number, and check number.

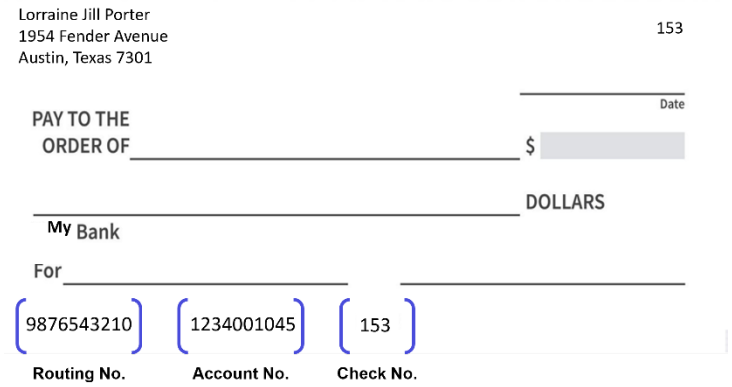


Figure 2 Counterfeit Check Example

The fraudster circulates the items for deposit in various ways and then extracts funds from the account if undetected.

Prevention Tips for Customers

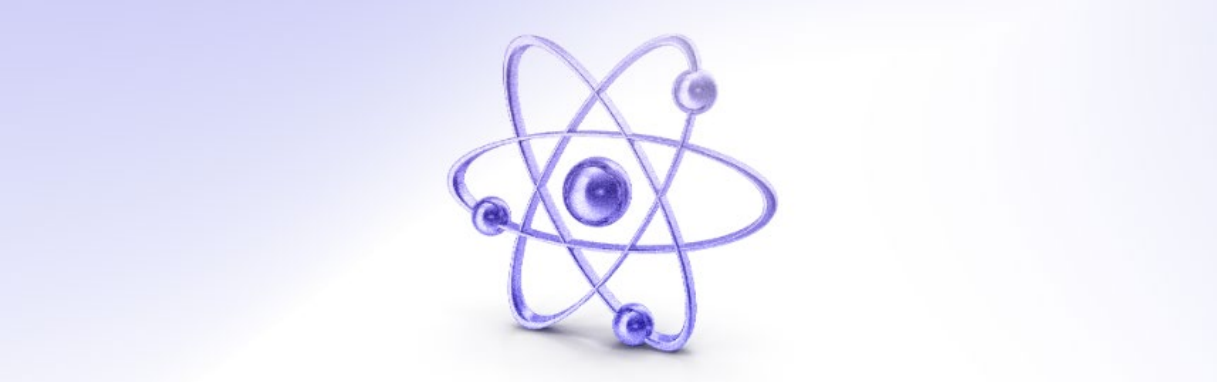
Fraudsters prey on people who are desperate, naïve, or actively participating in a fraud scam. Educate customers to be alert to phishing scams that leverage their emotions.
For consumers receiving a check related to work from home job ads, activity - authenticate the check – (1) call the issuing bank to verify the account; and (2) call the issuer to verify that the check is real (using phone numbers from an independent source, not those printed on the check).

Stopping Fraud at the Teller Line

- Expand the influence of your fraud prevention program by communicating with front-line tellers and back-office processors about current check fraud scams in your area. Provide examples of real items in circulation and what they should do if they come across a counterfeit item.
- Ensure tellers understand the purpose of Know Your Customer requirement.
- Financial institutions can also help protect customers by verifying checks with the issuing bank, using check verification software, and implementing strict check cashing policies
- Train your tellers/cashiers/customer service representatives to identify potential fraudulent checks and the proper procedure if a fraudulent check is identified.
- Train tellers to look for behaviors that may indicate suspicious activity, such as nervousness, trying to rush the transaction, or other such behaviors. They may not always

indicate deception, but “gut feelings” may be accurate – encourage personnel to take their time verifying the check.
- Consider any available fraud software or databases that may help to deter loss.
- Consider investing in UV counterfeit detection scanners. These devices read hidden security features and can be used to check currency, traveler's checks, money orders, credit cards, driver's licenses, passports, and government checks.

Counterfeit check fraud is one way fraudsters monetize stolen customer information. Preventing fraud overall involves different cybersecurity, software, and training disciplines to limit the institution's financial risk.



THREAT INTELLIGENCE UPDATE

New York DFS Issues New Guidance on AI

The New York Department of Financial Services (DFS) shares guidance on addressing AI risks

Summary

On 16 October, the New York Department of Financial Services (NYDFS) issued new guidance to assist regulated entities in addressing and combating cybersecurity risks arising from artificial intelligence (AI). The Guidance highlights four main cybersecurity threats related to the use of AI: AI-enabled social engineering, AI-enhanced cyber-attacks, exposure to theft of vast amounts of nonpublic information, and increased vulnerabilities due to third-party, vendor, and other supply chain dependencies.

To exemplify the threat of AI-enhanced cyber-attacks, this week OpenAI published a report detailing how threat actors used ChatGPT for debugging and developing malware, spreading misinformation, evading detection, and conducting spear-phishing attacks. Though the latter two threats may not yet fully come to fruition, they build upon existing data theft and third-party vendor risks experienced by institutions.

In addition to outlining the main cyber threats posed by AI, the NYDFS Guidance provides a list of recommended controls and measures for financial institutions – including access controls, cybersecurity training, and data management – designed to mitigate AI-related cyber threats.

New White Paper Focused on Deepfakes in the Financial Services Sector

Whitepaper highlights risks for the financial service sector

Summary

FS-ISAC’s Artificial Intelligence (AI) Risk Working Group produced a new white paper called *Deepfakes in the Financial Sector: Understanding the Threats, Managing the* Risks, which contains the first-ever Taxonomy of Deepfake Threats specifically for the financial service sector. Deepfakes are false but highly convincing video, images, and audio that threat actors use to infiltrate and steal from financial institutions. Written for both business and technical audiences, the Deepfake Taxonomy is categorized by threat – from CEO impersonations to attacks on deepfake detection models – and details the controls and mitigations appropriate to each threat. That approach enables firms to identify their greatest vulnerabilities and build bespoke defenses against this costly and growing threat.

The paper contains:

- How financial services institutions are likely to be attacked by deepfakes
- The assets threatened by deepfakes
- The primary recipients of deepfakes
- A summary of controls available to financial firms

JUST FOR COMMUNITY INSTITUTIONS

Board of Director Engagement in Cybersecurity Oversight

The frequency, speed, and sophistication of cyber-attacks lead NCUA to provide BOD directive

Summary

On 21 October, the National Credit Union Association (NCUA) released a letter to credit unions regarding a recent incident impacting a CU and four key areas that CU boards of directors should focus on. These four areas are:

1. Provide for recurring training
2. Approve Information Security program
3. Oversee operational management, specifically:

    - ***Internal and external communication***. Establish a communication strategy for informing your board immediately following a security incident, ensuring transparency and timely decision-making. The communication strategy should also inform both internal stakeholders and external parties, including your members and regulators, in the event of a cyber incident. Clear communication can help manage expectations and maintain trust.
    - ***Insurance considerations***. Evaluate cybersecurity insurance policies to ensure adequate coverage for potential incidents. This assessment includes understanding the scope of coverage and any exclusions that may apply.
    - ***Incident response team***. Identify and designate an incident response team that includes key personnel from various departments. This team should be prepared to take immediate action in the event of a cyber incident.
    - ***Tabletop exercises***. Conduct regular tabletop exercises to simulate cyber incident scenarios. These exercises will help your credit union board and management practice response plans, identify areas for improvement, and ensure that all team members understand their roles during an incident.

4. Incident response planning and resilience

By focusing on the key areas outlined above, your credit union's board of directors can significantly improve the credit union's cybersecurity posture and protect the interests of your members. Cybersecurity is not just an "IT" issue. It must be a critical component of any credit union's overall governance and risk-management strategy. A cyber incident can have far-reaching consequences, not only affecting your institution's financial stability but also potentially impacting the entire financial services system while eroding member trust and damaging your credit union's reputation.

By taking the proactive steps outlined above and prioritizing cybersecurity as a fundamental aspect of governance, your credit union's board of directors can effectively safeguard the credit union and its members' assets, maintain member trust, and ensure compliance with regulatory requirements. To that

end, we encourage you to consult the many available cybersecurity resources available on the NCUA's public website not just during Cybersecurity Month in October but also year-round.

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks
- Building Cryptographic Agility in the Financial Sector
- Protecting Financial Data with Encryption Controls
- Principles for Financial Institutions' Security and Resilience in Cloud Service Environments
- Business Information Security Officer (BISO) Program and Role
- Resilience in Action - Lessons from the Field
- Navigating Cyber 2024: Annual Threat Review and Predictions
- Digital Operational Resilience Act (DORA) Implementation Guidance
- Financial Services and AI: Leveraging the Advantages, Managing the Risks
- LockBit: Access, Encryption, Exfiltration, and Mitigation

See the full list of Knowledge Resources

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Recent Episodes

- Stephen Sparkes: The Evolution of the CISO Role
- Lindsey Bateman: Keep Your Eyes On The Horizon For Emerging Threats – And New Solutions
- Burim Bivolaku: Financial Sector Collaboration Is Key To Third-Party Risk Management
- Beate Zwijnenberg: Can Cyber Risk be Quantified?
- Josh Magri: The CRI Profile – A Simplified Approach To Better Assessment
- Phil Venables: AI in Cybersecurity - Threats, Toil, and Talent

UPCOMING EVENTS

Americas

- 27 - 30 October | Americas Fall Summit
- 18 November | November CIAC Webinar
- 4 December | Americas Member Success Session
- 9-12 March 2025 | Americas Spring Summit
- 3 June 2025 | FinCyber Today Canada

View all Americas events

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190