ACICE
ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 06/25 (Jun)

Security of Banks: Challenges in the Cyber Age

INTRODUCTION: INCREASING CYBER THREATS TO BANKS

1. Banks are often targeted by criminals seeking to steal money or disrupt economic activity, given the large amounts of money, sensitive data and transactions handled. According to the *International Monetary Fund (IMF)* Global Financial Stability Report in April 2024, attacks on financial firms account for nearly one-fifth of global cyber incidents, of which banks are the most frequent targets.

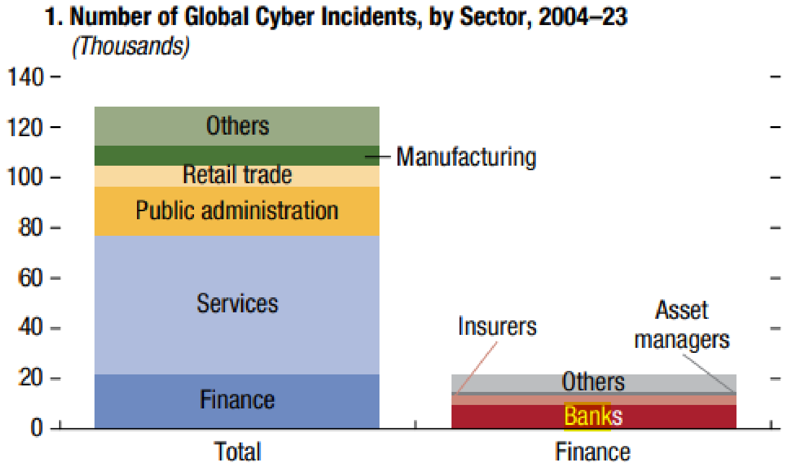


Fig. 1: Nearly one-fifth of global cyber incidents have affected the finance sector, of which banks are the most frequent targets. (Source: International Monetary Fund)

2. *Deloitte* reports that the COVID-19 pandemic spurred a rapid transition to greater digital connectivity, and many banks are struggling to address the cyber vulnerabilities and attacks introduced by a wider attack surface.

OVERWHELIMING ODDS: CYBER THREATS TO BANKS

Vulnerabilities in backend servers and networks

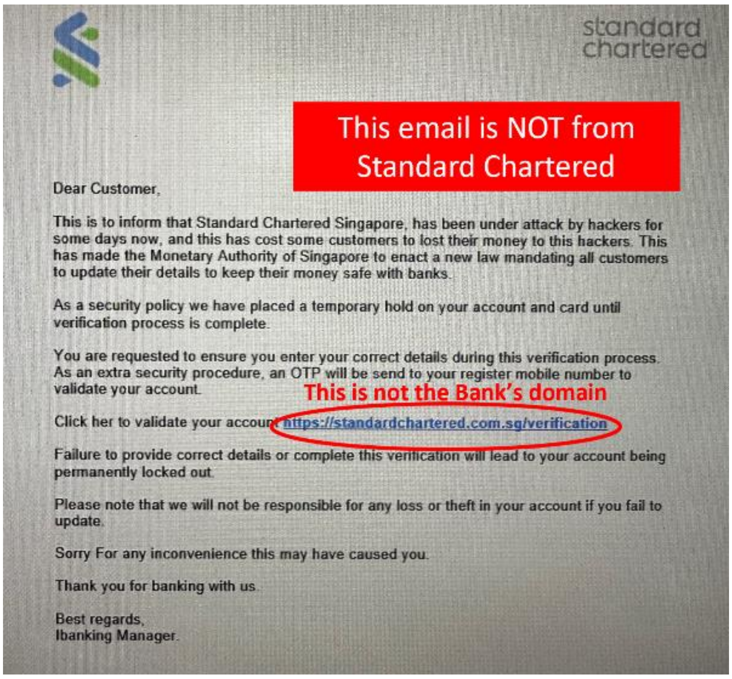
3. Backend servers and networks are used to facilitate banking transactions and store data in banks. According to *Boston Consulting Group*, many banks often lack a defined process for assessing cyber risk, resulting in the failure to identify where their systems are the most exposed. As a result, employees and even third-party vendors can access sensitive data on servers, potentially leading to information leaks or hacking.

Case in point:
In 2019, a former Amazon employee, Paige Thompson, developed a tool that scanned Amazon Web Services (AWS) for misconfigured accounts, allegedly to enrich herself financially and to earn bragging rights. Misconfigured accounts lack or have inappropriate security settings, resulting in vulnerabilities such as unrestricted access to information. Thompson leveraged these accounts to gain access to the systems of dozens of AWS customers, including Capital One, an American bank whose web application firewall for servers was misconfigured. The breach happened in March and April of 2019, but Capital One was allegedly not aware of the problem until mid-July, when someone tipped the company to a public GitHub page where the names, birth dates, social security numbers and email addresses of over 100 million customers were available. Capital One has since been fined $80 million for allegedly failing to secure users' data.

4. In the case of a catastrophic cybersecurity breach, standard disaster recovery planning may not be robust enough as connection between backup sites designed to replicate data to ensure continuity of service in banks can also rapidly replicate malware across technology.

Customer users' interface vulnerable to phishing activity

5. Phishing scams mimic any known website or email address. By creating urgency, scammers trick bank customers into clicking on phishing links. Stolen banking credentials can then be used to facilitate financial crime and lead to financial losses. In the case of a phishing scam on Standard Chartered accounts (Fig. 2), one would be able to spot signs of phishing. These include grammatical errors, links that closely resemble a company's official domain with minor differences in spelling, and claims that create a sense of urgency, such as the threat of the bank account being permanently locked.



standard chartered

This email is NOT from Standard Chartered

Dear Customer,

This is to inform that Standard Chartered Singapore, has been under attack by hackers for some days now, and this has cost some customers to lost their money to this hackers. This has made the Monetary Authority of Singapore to enact a new law mandating all customers to update their details to keep their money safe with banks.

As a security policy we have placed a temporary hold on your account and card until verification process is complete.

You are requested to ensure you enter your correct details during this verification process. As an extra security procedure, an OTP will be send to your register mobile number to validate your account.

This is not the Bank's domain

Click her to validate your account https://standardchartered.com.sg/verification

Failure to provide correct details or complete this verification will lead to your account being permanently locked out.

Please note that we will not be responsible for any loss or theft in your account if you fail to update.

Sorry For any inconvenience this may have caused you.

Thank you for banking with us.

Best regards,
Ibanking Manager.

Fig. 2: A sample of a phishing scam mimicking a Standard Chartered notice (Source: Standard Chartered)

6. Phishing-as-a-service (PhaaS) platforms also sell phishing templates for scammers' use, amplifying the ability of scammers to carry out phishing scams for financial benefit. For example, a sophisticated PhaaS network, BulletProftLink, sold clients fake login pages for websites. According to cybercrime intelligence company *Intel471*, these included login pages for financial institutions including American Express, Bank of America, Consumer Credit Union and Royal Bank of Canada.

7. *Intel471* also reported that BulletProftLink appeared to have more than 8,138 active clients and 327 phishing pages templates as of April 2023. In November that year, Royal Malaysian Police, with the aid of the Australian Federal police and the US FBI, finally shut down BulletProftLink after tracking it for years. Royal Malaysia Police seized servers, computers, jewellery, vehicles, and cryptocurrency wallets containing about 1 million Malaysian ringgit (about US$213,000) – illustrating the extent of the PhaaS operation.

ATMs – another attack vector

8. Automated Teller Machines (ATMs) are vulnerable to attacks, primarily due to outdated software and hardware – many ATMs still run on old, unsupported versions of Windows like XP or Windows 7, which was discontinued in 2020. These operating systems no longer receive security updates from Microsoft, leaving them exposed to known vulnerabilities that can be exploited by hackers. To migrate to new operating systems, however, older ATMs may require a new computer processor because the existing hardware lacks the horsepower to operate the more advanced software. In some instances, these newer processors are a different size than the old one, and will not even fit into the existing ATM, meaning that ATM providers must replace the entire ATM if they wish to upgrade.

9. As a result, the lack of software upgrading creates vulnerabilities, which, according to *NVISO Labs*, include:

a. Lack of or insufficient network access control. An attacker who has been able to connect to the ATM network via Ethernet can communicate with other systems on the same network, allowing the attacker to perform actions such as a network-driven cash-out.

b. Unencrypted communication to the backend server. An attacker who has hacked into the software can read sensitive transaction data and manipulate it to issue malformed funds.

c. Lack of or insufficient authentication to the exposed ATM network service. Spoofed backend commands that can surpass authentication checks can be sent to the exposed ATM service to make it cash out.

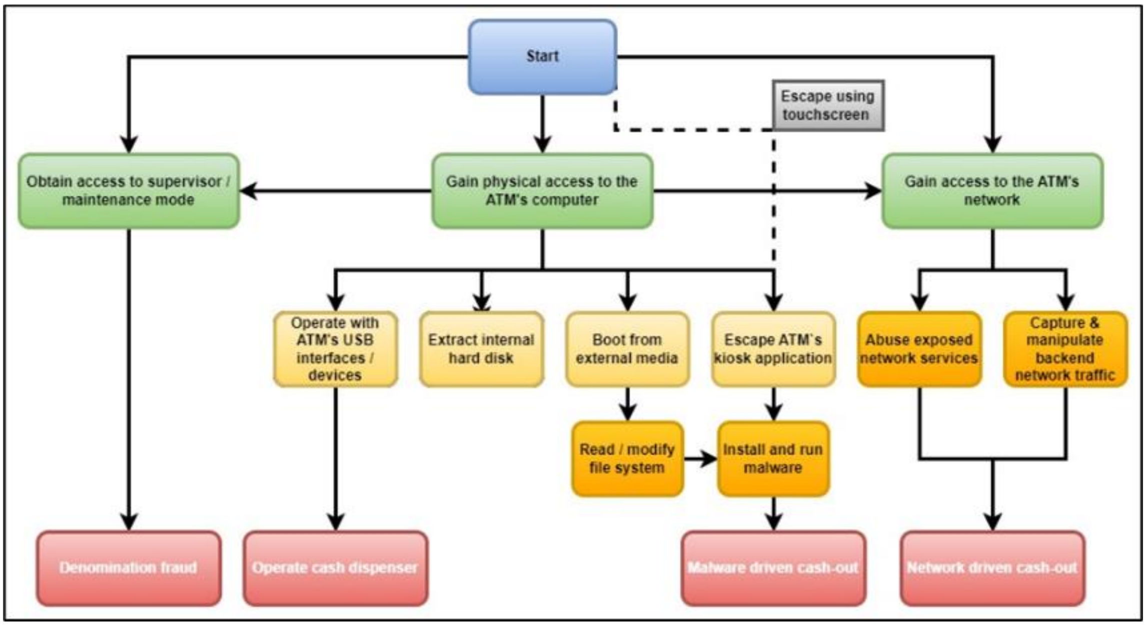

Start
Escape using touchscreen
Obtain access to supervisor / maintenance mode
Gain physical access to the ATM's computer
Gain access to the ATM's network
Operate with ATM's USB interfaces / devices
Extract internal hard disk
Boot from external media
Escape ATM's kiosk application
Abuse exposed network services
Capture & manipulate backend network traffic
Read / modify file system
Install and run malware
Denomination fraud
Operate cash dispenser
Malware driven cash-out
Network driven cash-out

Fig. 3: Flowchart of potential attack scenarios on ATMs (Source: NVISO Labs)

Case in point:
One of the most popular attack types is the Man-in-The-Middle (MiTM) attack, where an attacker infiltrates the server network, then secretly relays and possibly alters the communications between the ATM and the main server. By relaying information to the ATM whilst pretending to be the main server in an MiTM attack, a hacking group specializing in ATM compromise in India was able to extract the equivalent of up to $300,000 USD in 2021.

10. Criminals also physically tamper with ATM hardware, such as installing card skimmers that steal customer card data and PINs, which can be used to facilitate phantom withdrawals. This is still a popular method by criminals to gain cash from ATMs – the *Communications Fraud Control Association (CFCA)* found in their Global Fraud Loss Survey 2023 that there were over 18,000 physical attacks on ATMs globally.

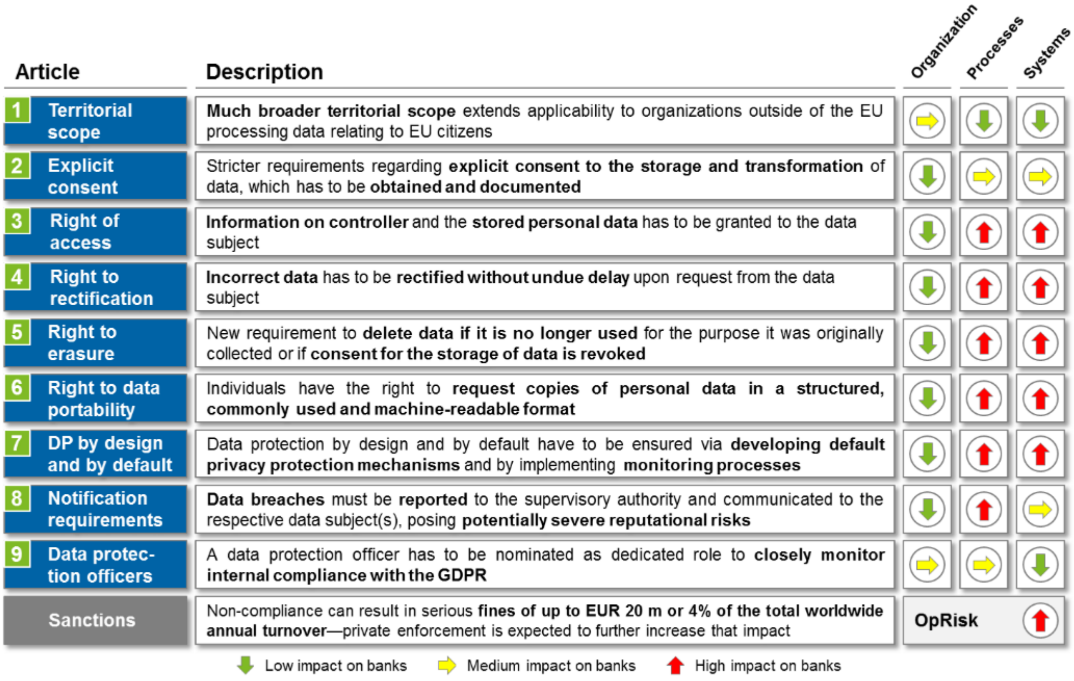
OVERCOMING THE ODDS: STRENGTHENING THE BANKS

Strengthened legislation and regulatory frameworks

11. Legislation and regulatory frameworks by governments can greatly increase the accountability of banks in case of cyber lapses and encourage banks to put in place stronger cybersecurity measures to protect customers' assets and data.

12. For example, the European Commission adopted the General Data Protection Regulation (GDPR) in 2016. It increased the regulatory requirements related to customer and counterparty data protection by strengthening and unifying the data protection regulation within the European Union. This includes notification requirements, where data breaches must be reported to the supervisory authority and

communicated to the respective data subject(s), posing potentially severe reputational risks.



Article	Description	Organization	Processes	Systems
1 Territorial scope	**Much broader territorial scope** extends applicability to organizations outside of the EU processing data relating to EU citizens	⇨	⬇	⬇
2 Explicit consent	Stricter requirements regarding **explicit consent to the storage and transformation** of data, which has to be **obtained and documented**	⬇	⇨	⇨
3 Right of access	**Information on controller** and the **stored personal data** has to be granted to the data subject	⬇	⬆	⬆
4 Right to rectification	**Incorrect data** has to be **rectified without undue delay** upon request from the data subject	⬇	⬆	⬆
5 Right to erasure	New requirement to **delete data if it is no longer used** for the purpose it was originally collected or if **consent for the storage of data is revoked**	⬇	⬆	⬆
6 Right to data portability	Individuals have the right to **request copies of personal data in a structured, commonly used and machine-readable format**	⬇	⬆	⬆
7 DP by design and by default	Data protection by design and by default have to be ensured via **developing default privacy protection mechanisms** and by implementing **monitoring processes**	⬇	⬆	⬆
8 Notification requirements	**Data breaches** must be **reported** to the supervisory authority and communicated to the respective data subject(s), posing **potentially severe reputational risks**	⬇	⬆	⇨
9 Data protection officers	A data protection officer has to be nominated as dedicated role to **closely monitor internal compliance with the GDPR**	⇨	⇨	⬇
Sanctions	Non-compliance can result in serious **fines of up to EUR 20 m or 4% of the total worldwide annual turnover**—private enforcement is expected to further increase that impact	**OpRisk**		⬆

⬇ Low impact on banks ⇨ Medium impact on banks ⬆ High impact on banks

Fig. 4: Overview of selected GPDR requirements, and their anticipated impact on banks (Source: BankingHub by zeb)

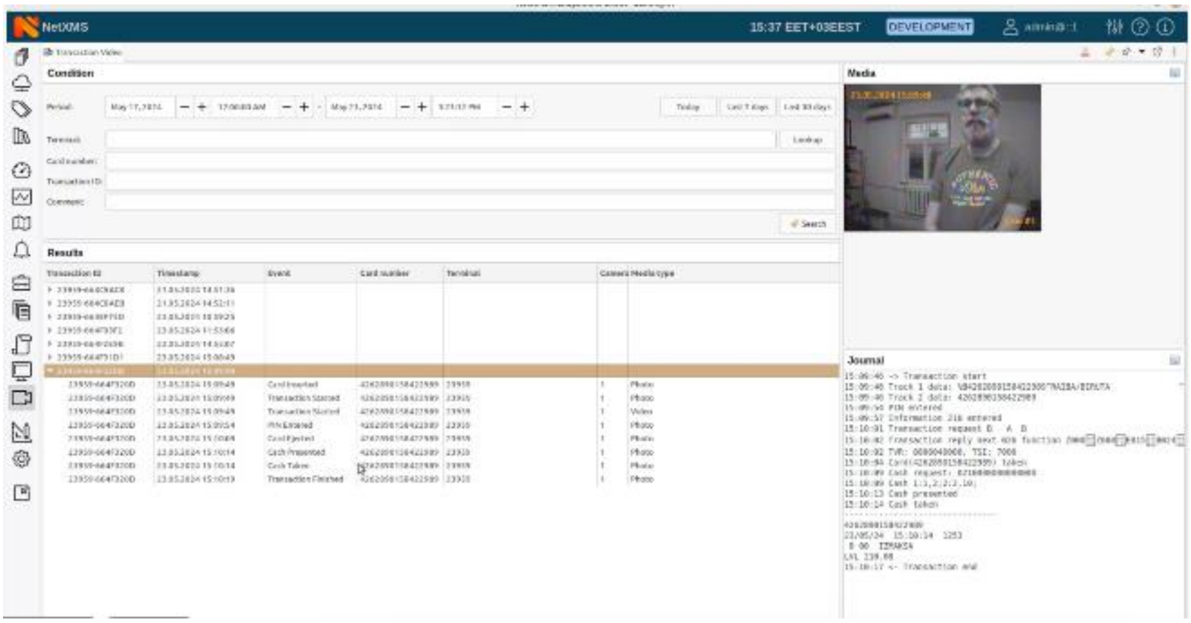
13. Regulatory authorities can also urge banks to use practices that better protect customers. To protect customers from phishing scams, the Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS) announced in July 2024 that major retail banks in Singapore would progressively phase out the use of OTPs for bank account login by customers who are digital token users.

Best Practices

14. To protect its servers and networks, banks should establish a regular schedule for applying security patches. These are updates released by software vendors to address vulnerabilities in their systems, and includes operating system updates, application updates, security software updates, and firewall updates.

15. Banks can also publish their official domains and sub-domains online so that customers can easily verify if they are entering an authentic website. Advice on steps to take if one has been scammed can also help victims prevent themselves from losing funds, such as by activating their account kill-switch automatically or via a hotline.

16. Banks can also use existing technological solutions to monitor and manage their systems. These can include using machine learning to identify anomalous behaviour, such as unusual cash withdrawals, which are immediately flagged to bank security teams for investigation. Banks can also use IT solutions for real-time monitoring and management solutions for ATMs, integrating transaction logs and video surveillance to remove inefficiencies that arise from manual cross-checking.



Transaction ID	Timestamp	Event	Card number	Terminal	Camera	Media type
▸ 23959-664C9ACE	21.05.2024 14:51:38					
▸ 23959-664CEAEB	21.05.2024 14:52:11					
▸ 23959-664EF75D	22.05.2024 10:09:25					
▸ 23959-664F93F1	23.05.2024 11:53:06					
▸ 23959-664F2[illegible]	22.05.2024 14:33:07					
▸ 23959-664F31D1	23.05.2024 15:00:49					
▾ [illegible]	[illegible]					
23959-664F320D	23.05.2024 15:09:49	Card Inserted	4262090158422989	23959	1	Photo
23959-664F320D	23.05.2024 15:09:49	Transaction Started	4262090158422989	23959	1	Photo
23959-664F320D	23.05.2024 15:09:49	Transaction Started	4262090158422989	23959	1	Video
23959-664F320D	23.05.2024 15:09:54	PIN Entered	4262090158422989	23959	1	Photo
23959-664F320D	23.05.2024 15:10:09	Card Ejected	4262090158422989	23959	1	Photo
23959-664F320D	23.05.2024 15:10:14	Cash Presented	4262090158422989	23959	1	Photo
23959-664F320D	23.05.2024 15:10:14	Cash Taken	4262090158422989	23959	1	Photo
23959-664F320D	23.05.2024 15:10:19	Transaction Finished	4262090158422989	23959	1	Photo

```
15:09:46 -> Transaction start
15:09:46 Track 1 data: %B4262080158422989^NAIBA/EDMUTA
15:09:46 Track 2 data: 4262898158422989
15:09:50 PIN entered
15:09:57 Information 216 entered
15:10:01 Transaction request D  A  D
15:10:02 Transaction reply next 026 function [illegible]
15:10:02 TVR: 0000040000, TSI: 7000
15:10:04 Card(4262808158422989) taken
15:10:09 Cash request: 0210000000000000
15:10:09 Cash 1:1,2:2,3,10;
15:10:13 Cash presented
15:10:14 Cash taken
----------------------------------
4262808158422989
23/05/24  15:10:14  1253
 0 00  IZMAKSA
LVL 239.00
15:10:17 <- Transaction end
```

Fig. 5: Example of video monitoring while ATM transaction is in progress (Source: NetXMS)

FUTURE CHALLENGES

17. As technology advances, cybercriminal operations are likely to become more sophisticated in the future. Some are increasingly using Generative AI and Large Language Models (LLMs) to create more believable personas and impersonate public figures. This allows

scammers to personalise scams to be more convincing and harder to detect.

18. The rise of PhaaS has also amplified the nefarious use of stolen data. On top of selling phishing templates, BulletProftLink also used a "double theft" tactic, where credentials stolen by customers using the PhaaS service were also sent to a server controlled by the operators. This allowed BulletProftLink to maximise profits by selling victims' credentials in the cybercrime underground. The impact of a single data breach is therefore no longer isolated, as one's data could be accessed and even sold to other cybercriminals for nefarious uses.

CONCLUSION

19. As banks continue to digitalise their services, protecting assets and data from cybercriminals has become ever more important. Regulatory frameworks and cybersecurity practices in banking need to keep up with changing trends in the sector, to prevent increasingly sophisticated criminal operations from exploiting cyber vulnerabilities.

.....

CONTACT DETAILS

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

....

REFERENCES

1. Cybersecurity in Banking Sector: Importance, Threats, Challenges https://www.knowledgehut.com/blog/security/cyber-security-in-banking

2. Rising Cyber Threats Pose Serious Concerns for Financial Stability https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

3. Five ways banks can mitigate a catastrophic cybersecurity event https://www.deloitte.com/global/en/services/consulting-risk/perspectives/five-ways-banks-mitigate-catastrophic-cybersecurity-event.html

4. Cybersecurity in Banking: Threats, Solutions & Best Practices https://www.esecurityplanet.com/cloud/cyber-security-in-banking/

5. Former Amazon employee convicted over 2019 Capital One hack https://www.theverge.com/2022/6/18/23173727/former-amazon-employee-convicted-over-2019-capital-one-hack-paige-thompson

6. Former hacker sentenced for stealing computer power to mine cryptocurrency and stealing the personal information of more than 100 million people https://www.justice.gov/usao-wdwa/pr/former-hacker-sentenced-stealing-computer-power-mine-cryptocurrency-and-stealing

7. Seattle Tech Worker Arrested for Data Theft Involving Large Financial Services Company https://www.justice.gov/usao-wdwa/pr/seattle-tech-worker-arrested-data-theft-involving-large-financial-services-company

8. Capital One ordered to pay $80 million penalty for its role in a 2019 data breach https://www.theverge.com/2020/8/8/21359761/capital-one-80-million-fine-2019-data-breach

9. Banking’s Cybersecurity Blind Spot—and How to Fix It https://www.bcg.com/publications/2018/banking-cybersecurity-blind-spot-how-to-fix-it

10. All you want to know about Phishing - Standard Chartered Singapore https://www.sc.com/sg/fraud-scam/phishing/

11. Adrian Katong ran a one-stop shop for phishing scams. Here's how he was tracked down - ABC News https://www.abc.net.au/news/2024-08-01/adrian-katong-phishing-scams-network-bulletproftlink-malaysia/104118036

12. Police takes down BulletProftLink large-scale phishing provider https://www.bleepingcomputer.com/news/security/police-takes-down-bulletproftlink-large-scale-phishing-provider/

13. Why 85% of ATMs Are Vulnerable to Attacks: 8 reasons banks must improve monitoring https://netxms.com/blog/why-85-of-atms-are-vulnerable-to-attacks-8-reasons-banks-must-improve-monitoring

14. Windows 10 migration for ATMs: The Microsoft timer ticks again atmmarketplace.com/blogs/windows-10-migration-for-atms-the-microsoft-timer-ticks-again/

15. How hackers cashed out $300K from ATMs in India via ATM jackpotting https://www.securitynewspaper.com/2021/06/01/how-hackers-cashed-out-300k-from-atms-in-india-via-atm-jackpotting/

16. Malware-based attacks on ATMs – A summary – NVISO Labs https://blog.nviso.eu/2023/01/10/malware-based-attacks-on-atms-a-summary/

17. General Data Protection Regulation | BankingHub https://www.bankinghub.eu/finance-risk/general-data-protection-regulation#elementor-toc__heading-anchor-2

18. Banks in Singapore introduce new measures to strengthen resistance against phishing scams banks-in-singapore-introduce-new-measures-to-strengthen-resistance-against-phishing-scams.pdf

19. Safeguarding Banks With Security Updates, Patching, and Pen Testing | Exabeam https://www.exabeam.com/blog/compliance/safeguarding-banks-with-security-updates-patching-and-pen-testing/

20. Security Patch Management: A Crucial Aspect Of Banking IT Infrastructure https://yves-brooks.com/security-patch-management-a-crucial-aspect-of-banking-it-infrastructure/

21. AI-enabled Fraud: How Scammers Are Exploiting Generative AI | TRM Blog https://www.trmlabs.com/resources/blog/ai-enabled-fraud-how-scammers-are-exploiting-generative-ai

22. BulletProofLink Phishing Platform Dismantled - CyberMaterial https://cybermaterial.com/bulletprooflink-phishing-platform-dismantled/