HOW TO AVOID GETTING HACKED ON THE INTERNET

INTERNET SAFETY AND PERSONAL SECURITY REPORTS

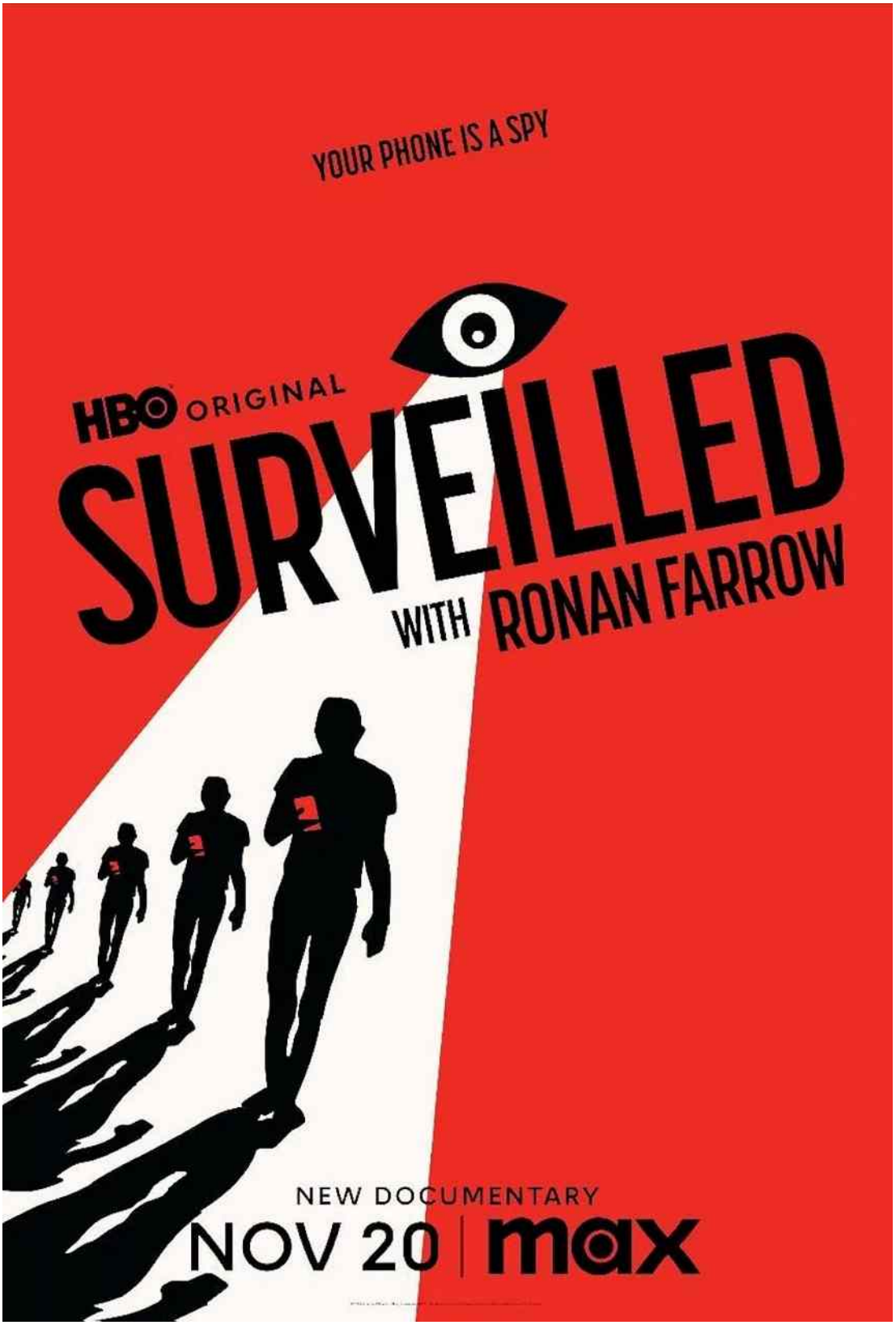
SEE THESE REPORTS COMPILED BY CONGRESSIONAL AND INTERNET SECURITY EXPERTS. YOUR MEDICAL RECORDS, BANKING RECORDS, CREDIT RECORDS, CREDIT CARD USES, DATING RECORDS, DMV REPORTS, PHONE TEXTS, HOME DATA, TAX RECORDS, UBER TRIPS AND ALL YOUR OTHER DATA HAVE ALREADY BEEN HACKED!

A PHONE OR WEB DEVICE GETS HACKED EVERY TWO SECONDS.
YOUR PHONE AND 'SMART DEVICES' HAVE THOUSANDS OF WAYS TO LET HACKERS IN. "THE CLOUD" = 'SOMEBODY ELSE'S COMPUTER', MOST OFTEN THOSE OTHER COMPUTERS ARE OPERATED BY YOUR ENEMIES. DON'T EVER PUT ANYTHING IMPORTANT ON THE INTERNET UNLESS IT IS STEALTHED.

IF YOU OWN A SMARTPHONE, EVERY APPLE AND ANDROID PHONE HAS THOUSANDS OF WAYS TO SPY ON YOU AND HARM YOUR PRIVACY. DON'T BE AN IDIOT - GET A 'DUMB PHONE' FLIP-PHONE.

FOLLOW THESE TIPS TO KEEP YOURSELF, AND YOUR FAMILY, SAFE!

SEE THE MOVIE: "SURVEILLED" BY RONAN FARROW, ON HBO MAX AND SEE HOW YOUR PHONE IS DESTROYING YOUR PRIVACY AND GIVING AWAY ALL YOUR SECRETS. GET RID OF YOUR 'SMART' PHONE!


YOUR PHONE IS A SPY
HBO ORIGINAL
SURVEILLED
WITH RONAN FARROW
NEW DOCUMENTARY
NOV 20 | max

Please share these documents with your friends and work-mates that are on the internet!

'I switched to flip phone and dramatically improved my well-being'...

More than 100 MILLION Americans' private information leaked in massive data breach at background check company

https://track.easypost.com/djE6dHJrX2UxZmI5OWQ2MDc2MTQ4OGJiNWE2NGEwODFjMTA1YjI2

BE SURE TO, ALSO, CHECK OUT THESE REPORTS ON THE RISKS OF USING SOCIAL MEDIA FROM THESE COMPANIES:

https://en.wikipedia.org/wiki/Criticism_of_Facebook

https://en.wikipedia.org/wiki/Criticism_of_Google

https://en.wikipedia.org/wiki/Criticism_of_Tesla,_Inc.

http://no-hack.org/THE ABYSMAL FAILURES OF ELON MUSK.pdf

https://campaignforaccountability.org/campaign-for-accountability-launches-google-transparency-project/

https://en.wikipedia.org/wiki/Criticism_of_Netflix

https://www.theguardian.com/news/2018/may/03/why-silicon-valley-cant-fix-itself-tech-humanism

https://www.forbes.com/sites/allysonkapin/2020/09/15/sexual-harassment-in-silicon-valley-still-rampant-as-ever/

https://www.makeuseof.com/tag/4-security-threats-whatsapp-users-need-know/

http://no-hack.org

http://http://san-francisco-dating.com

MORE CRUCIAL INVESTIGATION UPDATE DATA:

- AT&T says hacker stole data from 'NEARLY ALL' customers...
- One of biggest breaches in history!
- Parents urged to buy 'dumb' phones to protect children from socials...
- Privacy 'virtually impossible' on iPhones, experts warn...
- "Gay Furry Hackers" Attack Heritage Foundation And Release Sensitive Data
- AT&T Reveals Hackers Stole "Nearly All" Records Of Customer Calls, Texts
- Florida HIV results, social security numbers leaked online in huge data breach...
- Hackers leak data from nearly 10,000 internal DISNEY Slack channels...
- Massive Car Dealership Cyberattack Has Ended With A $25 Million Ransom
- UnitedHealth Group Projects Cyberattack Costs To Top $2.3B
- https://www.wired.com/story/secret-hunting-bill-demirkapi/
- Disney Faces Class Action Suit Over Massive Data Breach

Hackers have stolen the Social Security numbers of every American. How to protect yourself:

https://www.yahoo.com/news/hackers-may-stolen-social-security-100000278.html

https://www.bleepingcomputer.com/news/security/hackers-leak-27-billion-data-records-with-social-security-numbers/

Here is how Google rapes your privacy:

https://old.reddit.com/r/ProgrammerHumor/comments/1fl7bqy/thoughtyouwereinvisiblehuhthinkagain/lo0w6zy/

- **Water Facilities Warned to Improve Cybersecurity As Hackers Pounce...**
- **Kremlin-linked hackers claim cyberattacks on U.S., French, Polish water utilities...**
- **Furry hackers target far-right news outlet behind Kirk, Bannon...**
- **Furry hackers target far-right news outlet behind Charlie Kirk, Steve Bannon...**
- **FBI warns China hackers ready to 'wreak havoc' in USA...**
- **Hackers steal Russian prisoner database to avenge death of Navalny...**
- **Hackers steal Russian prisoner database to avenge death of Navalny....**
- **Biden admin to accuse Chinese hackers of targeting US companies...**
- **Water utilities targeted by foreign hackers, prompting calls for cybersecurity overhaul...**
- **Self-proclaimed 'gay furry hackers' breach nuke lab...**
- **Self-proclaimed 'gay furry hackers' breach nuclear lab...**
- **Hackers stole million people's DNA. What will they do with it?**
- **Pro-Hamas hackers send fake rocket alerts, knock sites offline...**
- **Hackers make their mark...**
- **'Furry' hackers claim breached NATO; Leak 3,000 files...**
- **'Furry' hackers claim to have breached NATO, leak 3,000 files...**
- **HACKERS ATTACK ROYALS**
- **Hackers nab State Dept. emails...**
- **Hackers nab 60K State Dept. emails...**
- **Hackers nab 60,000 State Dept. emails in breach...**
- **Red hackers target STARLINK...**
- **HACKERS GAIN CONTROL OF CASINO CARD SHUFFLING MACHINE FOR**

CONTROL OVER GAMES...

- **For first time, USA lets hackers break into satellite in space...**
- **UPDATE: Chinese hackers breach email of Commerce Secretary and State Dept officials...**
- **Beijing Hackers Spied on State Dept...**

Chinese Hackers Spied on State Dept...

- **Beijing hackers breach U.S. govt email...**
- **Chinese hackers breach U.S. govt email through MICROSOFT cloud...**
- **Hackers selling ChatGPT account conversations on dark web...**
- **REDDIT Hackers Threaten to Leak Stolen Data...**
- **RUSSIAN HACKERS DEMAND RANSOM FROM ENERGY DEPT...**
- **RUSSIAN HACKERS DEMAND RANSOM FROM ENERGY DEPT**
- **Americans should prepare for cyber sabotage from hackers...**
- **Hackers infiltrated naval infrastructure...**
- **Hackers that triggered US alarm hit defense targets...**
- **Chinese hackers that triggered US alarm hit defense targets...**
- **MICROSOFT warns Beijing hackers attacked U.S. infrastructure...**
- **MICROSOFT warns China hackers attacked U.S. infrastructure...**
- **MSFT warns China hackers attacked U.S. infrastructure...**
- **Mass event will let hackers test limits of new technology...**
- **Hackers claim Israeli power outages...**
- **Hackers claim to be behind Israeli power outages...**
- **Europe Air-Traffic Agency Under Attack From Hackers...**
- **Inside sting operation to catch N Korea crypto hackers...**
- **Ukraine hackers dupe Kremlin commander wife into sending sultry snaps...**
- **Ukraine hackers dupe Russian commander wife into sending sultry snaps...**
- **In Wild Spree, Hackers Accessed Federal Law Enforcement Database...**
- **Feds 'hack the hackers' to bring down ransomware gang...**
- **Russian hackers suspected to be behind UK Mail cyber attack...**
- **Hackers access GUARDIAN salary, passport info...**
- **Hackers planted evidence on computer of jailed priest, report says...**
-

A class action lawsuit brought against background check company National Public Data (also known as Jerico Pictures) alleges the personal information of 2.9 billion individuals has made its way onto the dark web via a data breach.

National Public Data uses a process called ‘scraping’ to collect and store personally identifying data from non-public sources to carry out background checks on billions of people.

This means that sensitive information like social security numbers, full names, addresses, relative's information was exposed - and crucially, it also means the information was not given willingly to the company, and many victims may not know it was stored at all.

Named plaintiff Christopher Hofmann was alerted by his identity-theft protection service provider that his data was exposed and leaked onto the dark web. Cyber criminal group ASDoD had listed a database which claimed to have the personal data of the individuals for sale at $3.5 million.

Hofman and the plaintiffs accused NPD of negligence, breaches of fiduciary duty and third-party beneficiary contract, and unjust enrichment. Hofman is fighting for financial compensation, and for the NPD to segment data, conduct database scanning, employ a threat-management system, and appoint a third-party assessor to conduct an evaluation of its cybersecurity frameworks annually for 10 years.

The court has been asked to require NPD purge personal data of all affected individuals and to encrypt all collected information going forward.

If confirmed, this would be classified as one of the largest data breaches ever in terms of affected individuals - rivalling the Yahoo! 2013 breach which affected three billion customers - and what's worse is that it's not yet clear how the data breach occurred.

You're letting people track your iPhone - here's how to stop it

You may think your phone's location is completely private, but you probably didn't think to check this feature that could be letting others track you. Here's how to turn it off.

In the ever-evolving battlefield of cybersecurity, a new adversary has emerged from the shadows. Mandiant, a leader in cyber threat intelligence, has identified the threat group orchestrating the notorious Basta Ransomware attacks. This revelation marks a significant milestone in understanding and combating this sophisticated threat.

Black Basta is a ransomware group that has rapidly risen to prominence in the cyber threat landscape since its first appearance in April 2022. Known for its highly targeted and sophisticated attacks, Black Basta operates as a Ransomware-as-a-Service (RaaS) enterprise. It most recently made news for breaching over 500 organizations worldwide. Its victims have included critical infrastructure sectors, according to a joint report by CISA and the FBI.

The Black Basta Menace

First detected in April 2022, Black Basta operates as a ransomware-as-a-service (RaaS) variant, targeting organizations across North America, Europe, and Australia. With over 500 victims spanning critical infrastructure sectors, including healthcare, this ransomware group has quickly become a formidable foe.

Since its inception, Black Basta has been highly active, amassing over 500 victims as of May 2024. The group utilizes top-tier hacking forums such as Exploit and XSS to seek insiders within target organizations to facilitate administrative access to networks. The group primarily targets organizations in the United States, Japan, Canada, the United Kingdom, Australia, and New Zealand.

Modus Operandi: How Black Basta Strikes

Black Basta affiliates leverage a variety of tactics, techniques, and procedures (TTPs) to infiltrate and cripple their targets. They often gain initial access through phishing attacks, exploiting vulnerabilities in remote desktop protocol (RDP) services, or deploying malware via compromised email attachments. Once inside, they escalate privileges, disable security features, and deploy the ransomware, encrypting critical data and demanding substantial ransoms for decryption keys.

Initial Access

Black Basta employs several strategies to gain initial access to target networks:

- Spear-Phishing Campaigns: In its early campaigns, Black Basta used highly targeted spear-phishing emails to trick individuals into divulging their credentials or downloading malicious attachments.
- Insider Information: The group is known to use illicit forums like Exploit and XSS to recruit insiders within target organizations, offering significant financial incentives for network access.

- Buying Network Access: Black Basta has advertised on forums their intent to purchase corporate network access, collaborating with initial access brokers (IABs) to infiltrate target systems.

Mandiant's Breakthrough

Mandiant’s investigation into Black Basta revealed a well-coordinated operation with potential links to other notorious cybercrime groups. Their analysis indicated that Black Basta’s methods and infrastructure bear similarities to those used by the infamous Evil Corp, suggesting a possible collaboration or shared resources among these cybercriminal entities.

The Broader Impact

The healthcare sector has been particularly hard-hit by Black Basta, with several high-profile attacks disrupting operations and compromising sensitive patient data. The ransomware’s ability to target both private industry and critical infrastructure underscores the urgent need for robust cybersecurity measures and incident response strategies.

Mitigation and Defense

In response to this growing threat, cybersecurity agencies like CISA, the FBI, and HHS have issued joint advisories, providing detailed guidance on detecting and mitigating Black Basta’s attacks. Key recommendations include regular backups, multifactor authentication, network segmentation, and comprehensive employee training to recognize and report phishing attempts.

Escalating Threats in a Digitalized World

As we progress through the year, the cybersecurity landscape continues to evolve with increasing sophistication in attacks. The rapid digital transformation across industries has expanded attack surfaces dramatically, highlighting an urgent need for adaptive security measures. This analysis draws on insights from leading industry sources to outline significant cyber threats and propose effective strategies for resilience.

The Ransomware Continues

"Ransomware attacks have increased in frequency and ransom demands, leaving even the best-prepared organizations vulnerable," reports CRN. This year, critical infrastructure sectors have been targeted, causing extensive disruptions. To combat these threats, organizations need to enhance their cybersecurity frameworks with robust disaster recovery plans, advanced detection systems, and

comprehensive employee training to mitigate ransomware risks effectively. The current ransomware request is above $10 million for enterprise companies.

Notable Incidents:

1. Financial Services: JPMorgan Chase reported a sophisticated cyberattack that compromised the personal data of millions of customers. The breach involved a combination of phishing and advanced persistent threats (APTs), indicating a high level of premeditation and resource investment by the attackers.

2. Healthcare: Besides UnitedHealth, Blue Cross Blue Shield was also targeted, where attackers exploited vulnerabilities in web applications to access sensitive patient records. This incident highlighted the ongoing challenges within the healthcare sector to protect patient information against increasingly malicious cyber threats.

3. Technology: A major ransomware attack targeted Apple, leading to significant operational disruptions and a temporary shutdown of some services. The attackers encrypted critical data files and demanded a large ransom, showcasing the disruptive potential of ransomware attacks on tech giants.

4. Retail: Target experienced another major cybersecurity incident this year, with attackers accessing transaction records and credit card information of thousands of customers through compromised point-of-sale (POS) systems. The breach was linked to malware that had been undetected within their network for months.

5. Government: The U.S. Department of Energy suffered a data breach involving the unauthorized access and exfiltration of classified data about energy infrastructure. This cyber espionage episode underscored the national security implications of cyberattacks.

The Human Element: Phishing is a major problem.

The report from TechCrunch on "The Human Element: Critical Findings" highlights how social engineering, particularly phishing, continues to be a formidable threat in cybersecurity breaches across various organizations. Several notable companies were impacted by attacks that leveraged the human element, underscoring the vulnerability of employees to sophisticated phishing schemes.

Companies Affected by Phishing Attacks:

1. Facebook: A targeted phishing campaign compromised the personal data of thousands of users. Attackers sent seemingly legitimate security update emails that redirected employees to a malicious website designed to harvest login credentials.

2. Cisco: Employees received emails that mimicked internal communications, leading to the unauthorized access of sensitive proprietary data. This breach highlighted the sophistication of phishing attacks that can bypass traditional email filters and security protocols.

3. HSBC Bank: A phishing scam impacted several HSBC branches, where employees clicked on malicious links sent via email, leading to financial fraud. The emails appeared to come from trusted sources, like senior management, which prompted quick but misguided action by the recipients.

These incidents demonstrate that even well-established companies with robust security measures can fall victim to the subtleties of social engineering. Phishing remains one of the most effective methods for initial penetration in cyber-attacks due to its direct targeting of human vulnerabilities—namely, trust and habit. Each of these cases involved emails crafted to look incredibly authentic, making it difficult for employees to recognize their malicious intent without proper training and awareness.

Cyber Criminals Entry and Attack

When cyber attackers use phishing to gain access to login credentials (like usernames and passwords), their subsequent actions can vary widely based on their objectives and the sophistication of the attack. Here are some common strategies they might employ after gaining initial access:

1. Placing Malware in Backups: Attackers may attempt to infect system backups with malware as part of a more extensive ransomware campaign or to ensure persistence in the system. By corrupting backups, they make it harder for the victim organization to recover without paying a ransom. However, infecting backups specifically requires additional access and control over the backup systems, which might not always be directly achievable through initial phishing access unless the credentials obtained give broad administrative privileges.

2. Creating Back Doors: Establishing backdoors is a common goal for attackers who want sustained access to a victim's network. After gaining initial entry through phishing, they might install a variety of tools or scripts that allow them to bypass normal authentication processes to regain entry later, often undetected. These backdoors can be challenging to detect and may remain operational for a long time, enabling data theft, additional malware deployment, or further exploitation.

3. Expanding Access: Often, the initial access gained via phishing is just a foothold within the network. Attackers typically use this access to perform lateral movement—exploring the network to access more sensitive data or systems. This process might involve the escalation of privileges or exploiting other vulnerabilities within the network to deepen their access.

4. Data Exfiltration: If the attacker's intent is to steal data, gaining initial access through phishing might be followed by locating and exfiltrating sensitive data to an external server. This can include personal data, intellectual property, or corporate secrets, depending on what is accessible with the compromised credentials.

5. Disruption and Sabotage: In some cases, especially in politically motivated or highly targeted attacks, the goal might be to disrupt operations or damage systems. Here, attackers might use their access to sabotage systems, which could include damaging backups or other critical infrastructure to maximize impact.

Identity Theft: IBM's Stark Warning

IBM's X-Force Threat Intelligence Index notes, "There has been a 45% increase in identity theft incidents this year, spurred by large-scale data breaches." Organizations must strengthen their identity protection measures with technologies like multi-factor authentication, biometric data verification, and continuous monitoring to safeguard user identities effectively.

The current biometric systems only link that biometric, cell phone to your account for login. The problem is that a criminal can create an account with your name and new password and that phone biometric, logs then into the new account with your name on it. Nimbus-Key ID has advanced to True User Verification™ with their KYC/AI/Biometric registration process. The login is secured with DE-MFA® or dynamically encrypted multi-factor authentication in a QRcode and PIN (patented) and dynamic key issuance.

Insights from the World Economic Forum

The Global Risks Report from the World Economic Forum underscores the escalating challenges of cyber insecurity, emphasizing its persistent threat across various time horizons. This year, cyber risks such as malware, deepfakes, and misinformation are highlighted as critical concerns that could impact supply chains, financial stability, and democratic processes. As technological advancements, like generative AI, become more prevalent, they bring both opportunities and heightened risks, particularly in exacerbating cyber inequities between well-protected organizations and those more vulnerable.

There's a growing divide in cyber resilience, with larger organizations advancing their security measures while small to medium-sized enterprises lag due to resource constraints. This inequity is exacerbated by a significant talent shortage in cybersecurity, further challenging organizations' ability to secure themselves against increasingly sophisticated cyber threats. The report calls for concerted efforts to bridge these gaps through global cooperation and strategic investments in cybersecurity infrastructure and workforce development.

IBM's Economic Analysis

The IBM X-Force Threat Intelligence Index provides a comprehensive overview based on monitoring significant security events worldwide. It reports a 71% increase in cyberattacks involving stolen credentials and highlights that 32% of incidents involved data theft. The report emphasizes the shift from ransomware to malware targeting data theft as the primary cyber threat, urging the adoption of advanced identity and access management solutions across hybrid and multi-cloud environments. It also suggests leveraging AI technologies to improve detection and response capabilities and prepare for potential threats against AI systems as they become more prevalent.

Verizon's Vulnerability Exploitation Report

The Verizon Data Breach Investigations Report, analyzed by Skyhigh Security, reveals an evolving threat landscape. The report examines 30,458 security incidents, noting a significant shift from ransomware to extortion attacks, which involves stealing data and demanding payment to prevent its release. It highlights a decrease in ransomware but a sharp rise in extortion, emphasizing the growing sophistication of cyber threats. The report also details the persistence of human error as a major vulnerability, with social engineering attacks remaining a prevalent method for breaching security.

Artificial Intelligence now in criminal use.

1. Europol Anticipates A Rise in AI-Driven Cybercrime: This article from TechStory reports on a new Europol report that predicts an increase in AI-driven cybercrime due to the sophisticated online tools used by criminals. The rise is linked to the broader availability and capabilities of AI technologies that enhance the effectiveness of cyberattacks. Read more.
2. Cybercriminal abuse of generative AI on the rise: Insurance Business Magazine discusses a report from TrendMicro, which states that cybercriminals are rapidly adopting generative AI to commit crimes, with the technology's use developing at a fast pace. This report underscores the dual-use nature of AI technologies in the cyber realm. Read more.

3. AI and Cybercrime Trends: DW Observatory explores how AI technologies are increasingly being used both to commit and combat cybercrime. The article highlights the ongoing race between cybercriminals using AI to discover new vulnerabilities and cybersecurity professionals working to protect digital infrastructures. Read more.

Conclusion: Building a Resilient Future

The cybersecurity challenges underscore the need for organizations to embrace advanced technologies, foster continuous learning, and maintain vigilant security practices. By adopting a holistic approach to cybersecurity, businesses can enhance their defenses and stay ahead of threats in an increasingly complex digital environment.

References

1. CRN: [Ransomware Trends 2024](https://www.crn.com/news/security/2024-ransomware-trends)

2. TechCrunch: [Social Engineering in Cyberattacks](https://techcrunch.com/2024/social-engineering-cyberattacks)

3. https://www.techradar.com/pro/security/unitedhealth-confirms-major-cyberattack-says-hackers-stole-substantial-amount-of-patient-data

4. IBM: [X-Force Threat Intelligence Index 2024](https://www.ibm.com/security/data-breach/threat-intelligence)

5. https://www.weforum.org/publications/global-risks-report-2024/

6. Verizon Business: 2024 Data Breach Investigations Report / https://www.skyhighsecurity.com/industry-perspectives/takeaways-from-verizon-2024-data-breach-report.html

7. https://ieeexplore.ieee.org/abstract/document/10607393/

8. https://www.healthcaredive.com/news/change-healthcare-cyberattack-lawsuit-consolidation/712492/