abluvp
All your data belongs to you

White Paper

A Common Sense & Collaborative Approach to Information and Cyber Security

For more information visit us at
www.abluva.com or connect with us at
connect@abluva.com

Table of Contents

Executive Summary

In today's digital world, where cyber threats are getting more clever, it's crucial for everyone in a company to use common sense and work together to keep important information safe. This paper talks about why it's so important for people to be careful and smart in their daily work to avoid falling for tricks that could lead to data breaches. It also explains how everyone in a company, from the top to the bottom, has a role to play in keeping the organization's defenses strong.

> The average cost of a data breach was **$4.45 million** in 2023, the highest average on record.
>
> - IBM

The paper gives some simple tips for employees, like being careful when clicking on links, using secure browsing practices, and not downloading important data on personal devices. It stresses the idea that every person in the company should take responsibility for keeping sensitive information safe and following security guidelines. The paper also talks about the bad things that can happen if someone is not careful, like losing important data, damaging the company's reputation, and costing a lot of money. Overall, it shows how a mix of using common sense and working together can help companies stay safe in the digital world.

Introduction

81 % of confirmed breaches were due to weak, reused, or stolen passwords in 2022.

-LastPass

83 % of data breaches in 2022 involved internal actors.

- Verizon

As organizations navigate the complex and dynamic landscape of cyber threats, it is crucial to recognize the significance of integrating common sense practices into daily operations. Simultaneously, promoting a collaborative mindset among employees enhances the collective defense against potential threats. This paper delves into the risks associated with employee negligence, emphasizing the need for shared responsibility in mitigating the devastating consequences of data breaches.

Why is a Common-Sense Approach Vital in Cybersecurity?

Having defensive tools in place is a critical component of a robust cybersecurity strategy, but a common-sense and collaborative approach adds a crucial layer of protection. Human factors, such as phishing vulnerabilities and social engineering tactics, can often bypass automated defenses. A common-sense approach encourages employees to be vigilant and discerning, reducing the risk of falling victim to evolving cyber threats. Furthermore, a collaborative culture fosters adaptability, rapid response to emerging threats, and a holistic security mindset, ensuring that cybersecurity becomes an integral part of organizational operations. This approach is essential for addressing the human element, mitigating insider threats, ensuring compliance, and enhancing incident response capabilities, making the overall cybersecurity posture more resilient.

Human error was a major contributing cause in **95%** of all breaches.

— IBM Cyber Security Intelligence Index Report.

Emails were the root cause of **30%** (with rounding) of attacks: **18%** started with a malicious email and **13%** with phishing.

- By Sophos The State of Ransomware 2023 Report.

Why is a Common-Sense Approach Vital in Cybersecurity?

In a rapidly changing threat landscape, having a defensive tool alone may not suffice to safeguard an organization's information assets. A common-sense and collaborative approach empowers employees to be proactive in identifying and mitigating security risks, complementing the capabilities of defensive tools. This proactive engagement, coupled with ongoing education creates a more comprehensive defense against a wide array of threats, ultimately contributing to a resilient and adaptive security posture for the organization.

Globally, **60%** of CISOs in agreement that human error is their organization's biggest cyber vulnerability worldwide in 2023.

-By Statista

Common Sense Measures

1. Think Before You Click

Employees should exercise caution when clicking on links, especially from unknown or suspicious sources. Verifying the target URL before clicking and confirming the legitimacy of the sender reduces the risk of falling victim to phishing attacks.

Use tools or services that expand shortened URLs to reveal the actual destination before clicking. E.g. *GetLinkInfo*.

Refrain from clicking on pop-up ads or unexpected windows, as these may be attempts to install malware or gather sensitive information.

2. Keep your personal accounts to yourself

Strictly prohibit the use of personal accounts for storing confidential information. This includes not only personal email accounts but also cloud storage and other online platforms.

Company-approved and secured systems should be the sole repositories for sensitive data.

E.g. All code must be stored exclusively in the official Git repository, and any storage in private repositories is strictly prohibited to maintain confidentiality and code integrity.

4. Browse safely with HTTPS and plugins

Utilizing HTTPS when browsing ensures encrypted communication between the user and the website, reducing the risk of data interception. Additionally, deploying browser plugins like *uBlock Origin* helps block malicious content, enhancing overall browser security.

3. Avoid Downloading Confidential Data on Personal Storage

Downloading sensitive information on personal devices introduces unnecessary risks.

Employees should be educated on the potential threats associated with unauthorized data storage and encouraged to use only approved, secure storage solutions.

5. Never use the Company's Email for a free trial

Using a company email address as a universal login for free trials poses security risks which may lead to increased susceptibility to phishing attacks, unauthorized access, and potential compromises of corporate credentials.

Use a temporary email address from websites like *temp-mail.org.*

> *"**1** out of **3** people took a risky action (such as clicking links or downloading malware) when faced with an attack."*
>
> - Proofpoint

Common Sense Measures

6. Safeguard Sensitive Information

Avoid revealing sensitive information, including passwords, privileged access details, secret keys, and API keys, to any individual in any situation.

9. Follow Secure Storage Practices

Avoid documenting or recording sensitive information on any tangible or digital media that may be accessible to unauthorized individuals.

If you handle physical documents containing sensitive information, store them securely and lock them away when not in use.

7. Opt-In For Browser Security Features.

Make sure that browsers are updated to the latest version to take advantage of built-in security features.

some browsers automatically block access to known malicious websites.

10. Multi-Factor Authentication

Enable multi-factor authentication (MFA) wherever possible to add an extra layer of security to your accounts.

8. Adherence to PoLP (Principle of Least Privilege)

Adhere to the Principle of Least Privilege (if you are a manager or have authority to grant or assign privilege), ensuring that user accounts and entities possess only the necessary access permissions required to fulfill specific tasks.

11. Create Complex Password

Create strong, unique passwords for each account and update them regularly.

Recommended to create Passphrases. Passphrases boast greater length compared to the typical password, rendering them more resistant to cracking attempts and thereby enhancing the overall security of a user's account.

Store account keys and passwords securely, preferably in a vault like AWS Secrets Manager, or use password-less authentication methods such as IAM trust or OTP-based login, avoiding plain text storage or weak encoding completely

> *"In 2022, a staggering **34%** of all attacks were launched as Business Email Compromise (BEC) attacks. To make matters worse, a shocking **80%** of organizations that fell victim to BEC attacks didn't have a Multi-Factor Authentication (MFA) solution in place."*
>
> *-Arctic Wolf*

Common Sense Measures

12. Use Secure Wi-Fi Connections

Refrain from accessing sensitive information or company resources when connected to unsecured public Wi-Fi networks.

If you must use public Wi-Fi, connect through a VPN to encrypt your internet connection, providing an additional layer of security and helping to protect sensitive data from potential eavesdropping or unauthorized access.

13. Stay Informed About Phishing Techniques

Stay informed about common phishing tactics and the latest trends in social engineering attacks.

Attend cybersecurity awareness training sessions provided by your organization to enhance your knowledge.

14. Regularly Update Software and Systems:

Ensure that your operating system, antivirus software, and applications are regularly updated to patch security vulnerabilities.

15. Report Suspicious Activity

If you suspect a phishing attempt or notice any suspicious activity, report it to your IT or security team immediately

> "**71%** of users don't change the default network name on work WI-Fi routers. "
>
> - Proofpoint

The Consequences of Employee Negligence

Data breaches resulting from employee negligence have become an unfortunate reality for many organizations. The havoc wreaked by such incidents can include:

Loss of Sensitive Information: Employee negligence can lead to the exposure of critical business data, intellectual property, and customer information.

Reputational Damage: The loss of trust from clients and stakeholders due to a data breach can have severe and lasting consequences on an organization's reputation.

Financial Impact: Remediation costs, legal fees, and potential fines stemming from a data breach can pose a significant financial burden on the affected organization.

56% of incidents experienced by organizations represented in this research were due to negligence, and the average annual cost to remediate the incident was **$6.6** million.

-Proofpoint

Operational Disruption: Data breaches often result in downtime, disrupting regular business operations and causing a cascading impact on productivity.

Loss of Business Opportunities: Organizations with a history of cyber incidents may struggle to win contracts or partnerships.

Increased Cybersecurity Costs: Companies may need to invest in advanced cybersecurity measures to prevent future incidents, increasing overall operational costs.

Case #1: Twitter User Scam: Phishing Scheme Involving Compromised Employees

What happened?

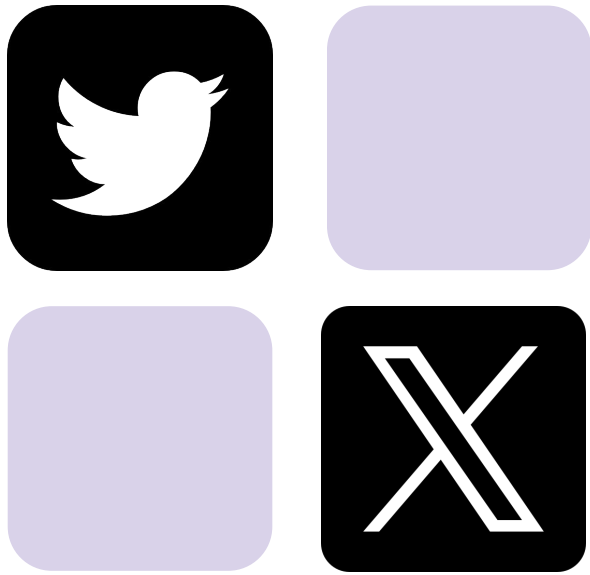
In July 2020, unauthorized individuals successfully breached the security of 130 Twitter accounts, encompassing both personal and corporate profiles with a minimum of one million followers each. These hackers exploited 45 of the compromised accounts to endorse a Bitcoin scam. Among the victims were prominent figures such as Barack Obama, Elon Musk, Bill Gates, Jeff Bezos, and Michael Bloomberg, as well as well-known entities like Apple and Uber.

What were the consequences?

Twitter users transferred a minimum of $180,000 in Bitcoin to fraudulent accounts, while the cryptocurrency exchange Coinbase prevented transfers totaling an additional $280,000. Following the event, Twitter witnessed a 4% decline in its stock price. In response, the company halted the rollout of its new API, focusing instead on enhancing security protocols and providing education to employees regarding social engineering attacks.

Why did it happen?

The incident occurred due to a series of spear phishing attacks targeting Twitter employees. Hackers meticulously collected information on staff members working remotely, reaching out to them while posing as Twitter IT administrators. Through these deceptive interactions, the attackers acquired user credentials. Subsequently, utilizing the compromised employee accounts, the hackers gained entry to administrator tools. With these tools at their disposal, they proceeded to reset the accounts of high-profile Twitter users, altering their credentials and posting fraudulent messages. This instance of an insider threat to cybersecurity underscores that Twitter failed to detect suspicious activities within the admin tools until the scam messages garnered attention from the press. Implementing User Entity and Behavior Analytics (UEBA) and Privileged Access Management (PAM) solutions could have bolstered the company's defenses, safeguarding access to admin tools and swiftly identifying unauthorized activities.



Consequences

- **4%** fall in stock prices
- Delay in new release
- Twitter users transferred a minimum of $180,000 in Bitcoin to fraudulent accounts.

Case #2: Mailchimp Experiences Triple Data Breach Due to Social Engineering

What happened?

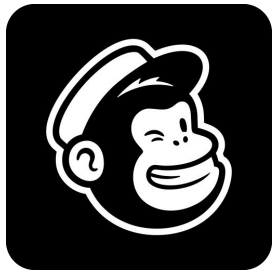
In 2022, Mailchimp and its associates fell victim to multiple cyberattacks. In January 2023, cybercriminals executed a successful phishing attack, deceiving at least one Mailchimp employee into revealing their credentials.

What were the consequences?

The data breach led to the compromise of a minimum of 133 Mailchimp user accounts. Among the affected accounts were those associated with businesses such as WooCommerce, Statista, Yuga Labs, Solana Foundation, and FanDuel.

Why did it happen?

The perpetrators directed their social engineering attacks specifically at Mailchimp employees and contractors. The success of these attacks hinged on an employee's inadvertence or failure to identify a social engineering attempt, enabling malicious actors to gain access to their user accounts. Instances of employee-induced data breaches highlight the importance of not underestimating the effectiveness of phishing and other social engineering techniques. Mitigating such risks necessitates ongoing cybersecurity training for both employees and partners, surpassing reliance solely on security software. Implementing a two-factor authentication (2FA) tool could have served as a preventive measure, as it requires an additional authentication factor and could have thwarted the successful use of compromised credentials by the attackers.



Consequences

- Loss of Reputation
- **133** Account compromised
- Loss of business opportunity

Conclusion

This white paper underscores the critical need for a common-sense and collaborative approach to information and cybersecurity, particularly in the face of escalating digital threats. It emphasizes the limitations of relying solely on automated defenses and highlights the significance of integrating human awareness into daily operations. By promoting vigilance among employees and fostering a shared responsibility for cybersecurity, organizations can enhance their resilience against evolving threats. The document provides practical measures, such as secure browsing practices, adherence to clear desk policies, and the Principle of Least Privilege, to mitigate insider threats resulting from employee negligence.

Real-world case studies, including the Twitter user scam and Mailchimp's triple data breach, vividly illustrate the severe consequences of employee-induced security lapses. These incidents led to financial losses, reputational damage, and operational disruptions, underscoring the urgency of proactive cybersecurity measures. The paper concludes that a holistic approach, encompassing both technological defenses and human-centric practices, is indispensable for creating a robust cybersecurity posture, safeguarding sensitive data, and mitigating the potentially devastating impact of data breaches on organizations.

> "When in doubt, pause, seek collaboration with knowledgeable individuals, and then choose the safest option guided by your instincts."

About Abluva

abluva
All your data belongs to you

For more information visit us at www.abluva.com or connect with us at connect@abluva.com

Abluva is a Palo Alto headquartered, research-focused, Data security startup. We are on the mission of enabling enterprises unlock the power of data by seamlessly embedding security into their ecosystems. Our team is taking head on the challenges posed by novel attack vectors and expanding attack surface across multiple data sources and public cloud environments. At the core of our approach are various contextual graphs that model deeper relationships of data and services. These relationships allows our multidimensional neural (and generative) networks to discover (and create) insights (and synthetic data).

References

Cost of a Data Breach Report 2023

2020 Twitter account hijacking - Wikipedia

11 Real-Life Insider Threat Examples - Code42

Personal data of 36,000 Boeing employees put at risk after employee emails info to spouse – GeekWire

2023 State of the Phish Report

The State of Ransomware 2023

CISO: Biggest cyber vulnerability is human error 2023 | Statista

2022 Cost Of Insider Threats Global Report