TECH BYTES

"Expert Strategies to Accelerate Your Business Efficiency, Simplify Operations, and Boost Profits"

INSIDE THIS ISSUE:

Our passion lies in technology and in assisting others.

Reach out for a friendly, no-pressure conversation today to explore how our team can enhance your data security and maximize the benefits of your current technology!

- **Matthew Dewees**
President

2024 STATE OF THE PHISH

Risky actions, real-world threats and user resilience in an age of human-centric cybersecurity.

Envision a cyberattack breaching your company's barriers. How does it unfold? Perhaps it's a deviously ingenious social engineering trap—a persuasive bait that ensnares the unsuspecting target. Or it could be a sophisticated technical maneuver that penetrates your security measures. However, in truth, attackers often find they don't need to exert such effort.

Security Behaviors and Attitudes

Even the most robust security measures can be compromised when users neglect fundamental practices like steering clear of dubious links, confirming the authenticity of the sender, and creating and confidentially maintaining a robust password. Regrettably, the disregard for these essential precautions by numerous users exposes both themselves and their organizations to potential threats.

End-user Behavior and Attitudes

Studies revealed that a significant 71% of participants admitted to engaging in risky behavior, with a staggering 96% acknowledging their awareness of the risks involved. Within this subset, 73% reported taking not just one, but multiple risky actions. Alarmingly, over a third of these actions were deemed by the respondents themselves as either 'extremely risky' or 'very risky.'

Why Risky Action is Taken

Participants are engaging in risky behaviors for several reasons, with the primary motivators being convenience, time-saving, and urgency. Interestingly, a minor segment of 2.5% were driven by curiosity to take risks. The findings underscore a crucial point: the issue isn't a lack of security awareness. In fact, individuals often consciously decide to take risks, even if it means jeopardizing the security of their organization.

Cybercriminals are acutely aware that human vulnerabilities can be exploited, whether due to negligence, lack of awareness, or, in rare cases, malicious intent. Our research indicates that social engineering plays a role in nearly every email threat we've analyzed. A notable 58% of users who admitted to taking a risky action also confessed to behaviors that expose them to fundamental social engineering schemes. These include actions like clicking on suspicious links, engaging with unknown senders, and sharing sensitive credentials with dubious entities. Such behaviors are gateways to serious cyber threats, including ransomware, malware, data breaches, and financial losses.

A contributing factor to users taking risks is the ambiguity surrounding accountability and responsibility for cybersecurity. Merely 41% of users recognize their role in maintaining cybersecurity at work. A small fraction, about 7%, outright deny any responsibility, whereas the majority, constituting 52%, remain uncertain about their role."

Attack Consequences

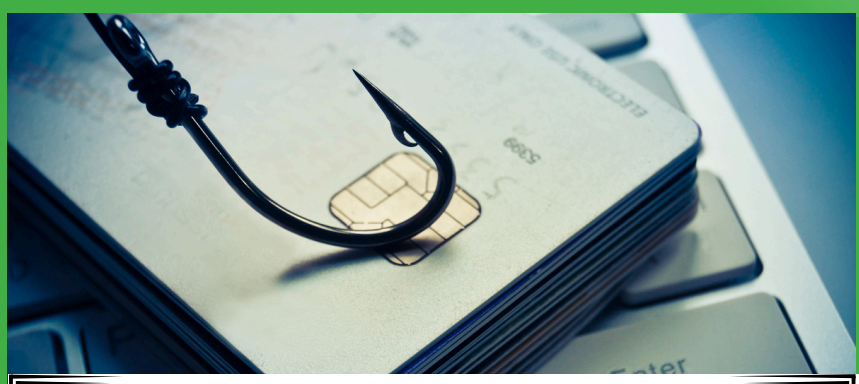
Phishing attacks can wreak havoc on an organization, inflicting severe financial and reputational harm. In 2023, 71% of organizations fell victim to at least one successful phishing attack, a decrease from 84% in the previous year. Despite this decline in attack frequency, the fallout has intensified. Reports of financial repercussions, including regulatory fines, surged by 144%, and instances of reputational damage climbed by 50% compared to the year before.

The cyber threat environment is in a state of perpetual change, with adversaries continually refining their strategies to gain the upper hand.

Areas for Improvement

Virtual DataWorks has partnered with Proofpoint to bring you, Phishing simulations - the solution that aligns organizational strategy with user behavior. Proofpoint simulations are not mere tests; they're educational tools that mirror the real-world threats lurking in your inbox.

Don't let the gap in perception become a breach in security. Choose Virtual DataWorks as your Proofpoint Partner to measure, understand, and enhance your cybersecurity awareness and resilience. Equip your team with the knowledge to spot and stop phishing attempts—because when everyone is vigilant, the entire organization stands stronger.



Empower Your Cybersecurity with Phishing Simulation Training

Don't leave your organization's safety to chance. Learn how Virtual DataWorks can equip your team with the knowledge to identify and neutralize phishing threats with Sophos Phishing Threat.

Virtual DataWorks

EXAMPLES OF HOW A DATA BREACH CAN COST YOUR BUSINESS FOR YEARS

The repercussions of a data breach extend far beyond the immediate aftermath. They often haunt businesses for years. Only 51% of data breach costs occur within the first year of an incident. The other 49% happen in year two and beyond.

The Unseen Costs of a Data Breach

Introduction to the First American Title Insurance Co. Case

The 2019 cybersecurity breach at First American serves as a stark illustration. It reminds us of the far-reaching consequences of a data breach. In this case, the New York Department of Financial Services (NYDFS) imposed a $1 million fine. Cybersecurity sites announced the fine in the fall of 2023. The company's fine was for failing to safeguard sensitive consumer information. This is one example of how costs can come long after an initial breach.

Lingering Impacts of a Data Breach

• Financial Repercussions

The financial toll of a data breach is significant. Immediate costs include things like:

- Breach detection
- Containment
- Customer notification

Beyond those, businesses face long-term expenses. These relate to legal battles, regulatory fines, and reparations.

• Reputation Damage

The impact on a business's reputation is arguably the most enduring consequence. Customers lose trust in a company's ability to protect their sensitive information. This loss of trust can result in a decline in customer retention. As well as acquisition difficulties and long-lasting damage to the brand image.

• Regulatory Scrutiny

Regulatory bodies increasingly hold businesses accountable for safeguarding consumer data. A data breach triggers regulatory scrutiny. This may lead to fines and ongoing compliance requirements.

• Operational Disruption

The aftermath of a data breach disrupts normal business operations. Companies must take remediation efforts and put in place enhanced security measures. These can divert resources away from core business functions.

• Customer Churn and Acquisition Challenges

A data breach often leads to customer churn. Individuals lose confidence in the business's ability to protect their data. Acquiring new customers becomes challenging. Potential clients are wary of associating with a brand that has suffered a breach. The prolonged effects on customer acquisition can hinder the company's growth as well as its market competitiveness.

A Cautionary Tale for Businesses Everywhere

The repercussions of a data breach extend far beyond the immediate incident. They can impact the financial health and reputation of a business for years as well as its regulatory standing.

ONLINE SECURITY: ADDRESSING THE DANGERS OF BROWSER EXTENSIONS

Browser extensions have become as common as mobile apps. People tend to download many and use few. These extensions offer users extra functionalities and customization options.

While browser extensions enhance the browsing experience, they also pose a danger which can mean significant risks to online security and privacy.

Key Risks Posed by Browser Extensions

• Privacy Intrusions
Many browser extensions request broad permissions. If abused, they can compromise user privacy. Some of these include accessing browsing history and monitoring keystrokes.

• Malicious Intent
There are many extensions developed with genuine intentions. But some extensions harbor malicious code. This code can exploit users for financial gain or other malicious purposes.

• Outdated or Abandoned Extensions
Extensions that are no longer maintained or updated pose a significant security risk. Outdated extensions may have unresolved vulnerabilities.

• Phishing and Social Engineering
Some malicious extensions engage in phishing attacks. These attacks can trick users into divulging sensitive information.

Mitigating the Risks: Best Practices for Browser Extension Security

1. Stick to official marketplaces.
2. Review permissions carefully.
3. Keep extensions updated.
4. Limit the number of extensions you install.
5. Use security software.
6. Educate Yourself.
7. Report Suspicious Extensions.
8. Regularly audit your extensions.

LEARN MORE

7 AI TRENDS THAT ARE SWEEPING THE CYBERSECURITY REALM

As cyber threats grow in sophistication, traditional measures face challenges in keeping pace. This is where AI steps in. It offers a dynamic and adaptive approach to cybersecurity.

Machine learning algorithms, neural networks, and other AI technologies analyze vast datasets. They do this at unprecedented speeds.

The integration of AI in cybersecurity doesn't replace human expertise. It enhances it.

AI Trends Sweeping the Cybersecurity Realm

1. Predictive Threat Intelligence
2. Behavioral Analytics
3. Autonomous Security Systems
4. Explainable AI (XAI)
5. Cloud Security Augmentation
6. Deception Technology
7. Zero Trust Architecture

THE NEWEST FEATURES OF MICROSOFT EDGE

Microsoft Edge continues to redefine user experiences. This is due to Microsoft's commitment to innovation. The latest updates bring a host of features. These are designed to enhance productivity, security, and browsing satisfaction.

From personalized workspaces to a built-in VPN, Microsoft Edge is not just a browser. It's a comprehensive toolkit for users navigating the digital landscape.

Virtual DataWorks has Partnered with Microsoft to bring you the newest Features of Microsoft Edge:

- Workspaces to organize browser session focuses
- Built-in Edge Secure Network VPN
- Autofill for more webform fields
- Web Capture
- Copilot (AI)
- Read Aloud

LEARN MORE

Secure Your Digital Horizon with Next-Gen Cybersecurity Solutions

Don't wait for a breach to rethink your security strategy. Partner with us and stay one step ahead of cyber threats.

By having a Managed Services Provider, like Virtual DataWorks, we will help you leverage your technology through a customized managed services program that allows us to:

- Monitor and maintain every device on your network
- Eliminate the need to troubleshoot problems on the network. By having them setup correctly and monitored you significantly reduce the number of "bandages" put in place by different IT providers.
- Have a team of of technicians watching your network's every move
- Give your employees access to our help desk. We are available 24/7.

Schedule A Free Consultation