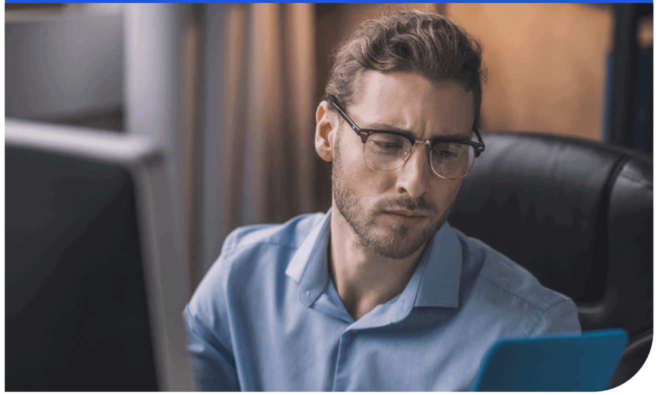
NATIVUC
CLOUD TECHNOLOGY MARKETPLACE

Outsmarting Cybercriminals: A Guide to Navigating Today's Cybersecurity Threat Landscape

What's Inside

In this guide, we will explore common cybercrime targets and how you can help your customers outsmart costly intruders.

What's Inside Your Guide



Introduction

Introduction

News headlines are filled with frightening tales of businesses suffering the costly consequences of growing cyberattacks. To understand the 2024 cybersecurity threat landscape, open any news site. The headlines are filled with frightening tales of banks, internet service providers, healthcare organizations, and other big players suffering the costly consequences of growing cyberattacks. And even though they may not make it on the news, the local insurance broker, bookkeeping service, and pharmacy on the corner are not immune.

Key Statistics

- **2,365** cyberattacks and **343,338,964** victims in 2023.[1]
- **72%** increase in data breaches from 2021 to 2023. 2021 held the previous record.[1]
- US cybercrime costs reached approximately **$320 billion** as of 2023, expected to hit **$1.82 trillion** by 2028.[2]

The growing rate of cyberattacks creates a great deal of "FUD": fear, uncertainty, and doubt. Many business owners ignore the risk to their organization and rely on hope and luck due to the complexity of cybersecurity. However, beginning a cybersecurity journey doesn't need to be overwhelming. By viewing their organization from the perspective of an attacker, business owners can identify gaps and take action. In other words: Think like a bad guy.

In this guide, we will explore common cybercrime targets and how you can help your customers outsmart costly intruders.

Understanding Common Cybercrime Targets

Understanding Common Cybercrime Targets

Even though it's against human nature, it's beneficial to examine your organization as a cybercriminal would. While it is always good to see the strengths of an environment, the bad guys are looking for the weaknesses. Here are some common cybercrime targets and ways to combat them:

1. Phishing and Untrained Staff

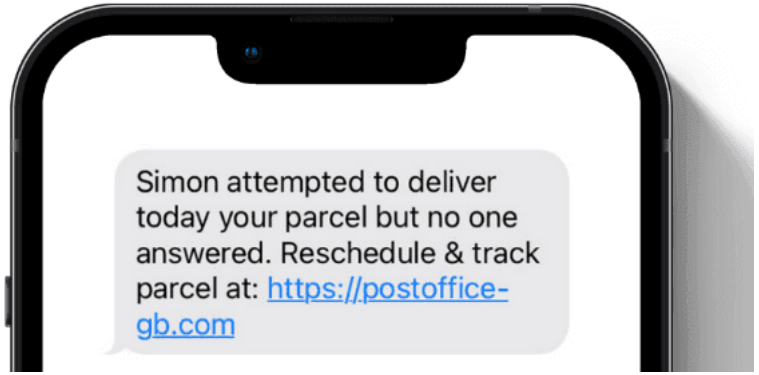
There is an adage that cybercriminals use: "We don't hack machines, we hack people." People are one of the weakest areas of an organization when it comes to cybersecurity. According to StationX, a leading provider of cybersecurity training and consulting, phishing is the most common form of cybercrime. Phishing involves sending scam emails or text messages that trick individuals into providing sensitive data or clicking malicious links. Over a trillion phishing emails are sent each year, and 36% of all data breaches involve phishing. [3]

Key Statistics

- **1 trillion+** phishing emails per year
- **36%** of all data breaches involve phishing

Combatting Phishing

Organizations should implement cybersecurity awareness training that includes phishing campaigns. It is essential that employees are educated in the techniques that the bad guys use, especially phishing. Security staff should send random (but innocuous) phishing simulations to all employees at various times. When a link in one of these emails is clicked, the user should be educated on what happened and how to better respond the next time a suspicious message appears. These emails should not be used to embarrass or make fun of anyone but only to educate.



Simon attempted to deliver today your parcel but no one answered. Reschedule & track parcel at: https://postoffice-gb.com

Tell-tale signs of a phishing message: Links that don't go to official websites. Do not be tempted to click!

2. Social Engineering and Unassuming Executives

CompTIA, a widely recognized IT trade organization, defines social engineering as “methods employed by hackers to gain the trust of an end user so that the hacker can obtain information that can be used to access data or systems." Social engineering typically involves impersonating representatives of legitimate organizations to manipulate people into supplying information such as passwords or personal details.[4]

Common Examples Include:

- **Spear-phishing:** Very targeted attacks against individuals within a business
- **Ransomware:** Malicious software which blocks access to a computer until a fee is paid
- **Pretexting:** Use of a fabricated story, or pretext, to gain a victim's trust and manipulate them into sharing sensitive information, sending money, etc.

Combatting Social Engineering

IT leaders need to take a close look at individuals within the company who have access to sensitive data, such as executive assistants, front office personnel, and helpdesk workers. Training them to recognize and not be afraid to question anything that doesn’t pass the “gut check” is critical. If these employees are hesitant, they should have the authority to escalate to management.

3. Cybersecurity Staff Shortages Create Unwanted Attention

CSO Online reports that the cybersecurity workforce shortage reached a record high of nearly 4 million, despite the cybersecurity workforce growing by almost 10% in the last year.[5]

This is a favorite "opportunity" of cyber criminals. All the bad guy needs to do is search their target company's job boards and identify open IT and cybersecurity positions. The more positions that are open and the older they are signal a staff shortage, and possibly an effortless way to make entry.

Combatting Staff Shortages

While solving workforce shortages can seem daunting there are many service providers that will take this headache on for IT leaders. Service providers can monitor systems 24/7, reducing the burden and cost of maintaining internal staff and infrastructure. Additionally, the capital costs involved in creating a Security Operations Center (SOC) and training staff to a level needed to discover, respond, and recover from today's increasingly complex incidents can add up.

4. AI-driven Cyber Threats and the Struggle to Keep Up

There is no doubt that the rise of artificial intelligence (AI) has taken the world by storm. While AI can do wonders for efficiency and productivity across an organization, the bad guys are using it in just as many ways for evil.

Among the most malicious applications: Cybercriminals use AI to create deepfake voices and impersonate corporate executives. CNN recently reported that a finance worker at a multinational firm was tricked into paying out $25 million to fraudsters who used deepfake technology to pose as the company's chief financial officer in a video conference call.[6]

Combatting Deepfakes

While deepfake technology is one of the most difficult attacks to counter, certain human elements cannot be forged. An effective way to outsmart deepfake videos or audio is to ask a question only the real person would know. For instance, if the target recently had dinner with the colleague the bad guy was imitating, they could ask a question about the restaurant, or the appetizer served. Simple human interactions like these can confuse even the most realistic forgeries.

Cybercriminals are also using AI to create new and harmful malware. This AI can test itself against security software to evade detection and find weaknesses in target systems, which cybercriminals use to plan and launch their attacks. This means that the malware can change its tactics during an attack, reacting to what it encounters to evade security measures more effectively. Additionally, “Dark LLMs”, the criminal version of ChatGPT, can break into systems and spread malware. These tools are often sold on the dark web, making malware invasions and other cybercrime more accessible and harder to predict.

Combatting AI-driven Malware

Organizations should adopt a multi-layered security approach that includes employing advanced machine learning detection technologies, strong encryption and multi-factor authentication, and maintaining diligent software updates. Regular security awareness training and a robust incident response plan are also crucial.

The Technology Advisor's Role in Successful Cybersecurity Strategies

The Technology Advisor's Role in Successful Cybersecurity Strategies

Now is the time for technology advisors to help organizations of all sizes navigate the complexities of advanced threats and get ahead of the bad guys. The NativUC 2023 Tech Trends Report revealed that most IT leaders are willing to engage with a new advisor, especially those who demonstrate profound knowledge of emerging technologies. And 85% of technology advisors surveyed predict cybersecurity solutions will see the greatest demand in the market in the next two years.[7]

Seize this opportunity to ask your customers if they would like some additional resources to help them in their cybersecurity journey.

You have access to top experts who can:

- Guide you on conversation starters
- Help you identify cybersecurity risks and gaps
- Make the right recommendations on the best advanced technology options available
- Empower you to discuss cybersecurity strategies with confidence

Technology advisors are seeing increased demand for cybersecurity

- **85%** of technology advisors indicated cybersecurity solutions will see the greatest demand in the next two years
- **50%** say their company should emphasize cybersecurity as the leading product

(2023 NativUC Tech Trends Report)

Conclusion

As more people conduct activities online and attacker techniques become more sophisticated, cyber threats have reached unprecedented levels. Ignoring these evolving threats will not reduce an organization’s attack surface; inaction will only make it more attractive to the bad guys. Companies must prioritize security preparedness by honestly assessing their risks, addressing them promptly, and recognizing that some aspects may require external help. NativUC's team of cybersecurity engineers and solution experts are well-versed in advanced technologies and hold the latest certifications such as CISSP, CISM, and CCSP. We provide the tools and expertise to identify the impact of loss, harm, and downtime on critical assets, prioritize mitigation activities, and identify third-party organizations to fill resource gaps. With access to top cybersecurity suppliers, you can offer solutions to your customers that replace fear and uncertainty with peace of mind.

Contact your NativUC Partner Development Manager today to learn how we can support your cybersecurity business and drive growth together.

Download PDF

About us

At NativUC, we believe that the future of business lies at the intersection of innovation, security, and human connection. As a leading provider of AI-driven solutions, we empower organizations to deliver exceptional customer experiences while safeguarding their digital ecosystems.

We specialize in:

AI-Powered Customer Experience: Helping businesses create seamless, personalized interactions that drive loyalty and growth.

Cybersecurity Solutions: Protecting organizations from evolving threats while ensuring compliance and trust.

Innovative Technology: Leveraging cutting-edge AI to transform how businesses connect with their customers and secure their operations.

Why Choose NativUC?

Proven Expertise: With years of experience in AI, CX, and cybersecurity, we've helped businesses across industries achieve measurable results.

Tailored Solutions: We understand that every business is unique. Our solutions are customized to meet your specific needs and goals.

Future-Ready Approach: We don't just solve today's challenges—we prepare you for tomorrow's opportunities.

Ready to transform your business? Let's connect and explore how NativUC can help you achieve your goals.

Talk to an expert today

Sources:

1. St. John, Maria. Forbes: *Cybersecurity Stats: Facts And Figures You Should Know.* 28 February 2024. <https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/#Sources?>.
2. Statista. *Estimated annual cost of cybercrime in the United States from 2017 to 2028.* 17 July 2023. <https://www.statista.com/forecasts/1399040/us-cybercrime-cost-annual>.
3. Smith, Gary. *Phishing Statistics.* 10 April 2024. <https://www.stationx.net/phishing-statistics/>.
4. CompTIA. *What is social engineering.* N.d <https://www.comptia.org/content/articles/what-is-social-engineering>.
5. Hill, Michael. CSO Onine: *Cybersecurity workforce shortage reaches 4 milion despite siginficant recruitment drive.* 31 October 2023. <https://www.csoonline.com/article/657598/cybersecurity-workforce-shortage-reaches-4-million-despite-significant-recruitment-drive.html>.
6. Chen, Heather and Kathleen Magramo. CNN: F*inance worker pays out $25 million after video call with deepfake 'chief financial officer'.* 2 April 2024. <https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>.
7. NativUC. *2023 NativUC Technology Trends Report.* <https://www.NativUC.com.au/resources/tech-trends-2023/>.