“Easter Eggs" for Cybersecurity:-Unraveling Hidden Gems to Protect Your Small Business

By: Scott Velmer

Around three-quarters (73%) of small businesses reported a cybersecurity attack in 2023, according to the Identity Theft Resource Center. Phishing continues to dominate as the most prevalent form of cybercrime, but ransomware threats continue to grow. Small businesses are bearing a substantial financial burden due to ransomware incidents, with U.S. enterprises shelling out more than $16,000 in cyber ransoms over the last year. As small businesses navigate the perilous landscape of cyber threats, it becomes imperative to equip themselves with effective defenses.

Small businesses must embark on a digital journey akin to an Easter egg hunt, unaware of lurking threats. As they navigate the virtual terrain, cyber adversaries lie in wait, ready to exploit vulnerabilities. The quest for business success is accompanied by the challenge of safeguarding sensitive data. Here, I’ll unveil Easter Eggs to be on the hunt for to fortify your defenses.

Easter Egg 1: The Hunt for Strong Passwords and Multi-Factor Authentication

Creating and managing strong passwords is akin to having a unique, uncrackable code for each egg in your Easter basket. Ensure your in-house and remote employees as well as your third party vendors and contractors know how to create strong passwords, including length, complexity, and the avoidance of common words or phrases. Explore the use of password managers and how they can aid in generating and storing complex passwords securely.

While strong passwords are one egg in your cybersecurity basket, it’s important to add multi-factor authentication (MFA) for an extra layer of protection as it acts as a vigilant sentinel. MFA can be added in different ways like SMS codes, authenticator apps, or biometric verification. Having the extra step of identifying the user is actually the user helps prevent unauthorized access, even if a password is compromised. According to Microsoft, implementing MFA reduces the likelihood you’ll get attacked by 99%.

Streamlining authentication with a single sign-on is a game-changer, reducing the hassle of managing multiple multi-factor authentications. Imagine it as the Easter Bunny managing a centralized identity basket, where each service, like Zoom or Microsoft, gets its own special authentication egg. Internally, we've adopted this with Microsoft, making it a seamless process. In the age of app-based authentication, consider using Microsoft's security app on your mobile device for MFA instead of relying on SMS codes, reducing the risk of interception.

Easter Egg 2: Enhance Your Phone’s Security

In our digital age, where smartphones are extensions of our daily lives, it's easy to overlook the importance of securing these personal devices against cyber threats. Often, we forget that our phones need robust protection in the realm of cybersecurity. One key tip, disable SMS authentication or phone number-based authentication, as they are especially vulnerable to SIM attacks. This is especially important when traveling internationally as SIM card vulnerabilities are more pronounced.

Modern devices, whether it's built-in or not, offer encryption capabilities. For instance, Microsoft utilizes a TPM chip, Mac has its proprietary system, and Android has its own approach. While specifics may vary, most modern devices provide a way to encrypt your data. To activate this feature, explore your device settings, whether it's on your phone or computer. The Easter egg is ensuring encryption is turned on for enhanced security. If unsure, you can search for instructions based on your device type. As for data encryption, explore your device settings to enable encryption for enhanced security or review these specific instructions for Android and Apple.

Safeguarding against cyber threats requires a comprehensive approach that goes beyond individual devices, encompassing the collective defense of an organization. This includes not only personal devices but also work phones and devices brought into the corporate environment through BYOD (Bring Your Own Device) initiatives. For robust organizational security, implement geolocation and geo-protection measures, limiting communication access from regions with no business relevance. This strategic approach acts as a formidable defense against various attacks, including AI-driven mass spamming. Incorporating these insights into employee training ensures widespread awareness and adoption of these crucial security practices. Additionally, when considering international travel, it's prudent to extend these measures, selectively enabling communication avenues only when necessary.

If unsure about implementing these strategies, seeking the expertise of cybersecurity professionals, like Vertilocity, is a wise choice to navigate the complexities and fortify your organization's cyber defenses effectively.

Easter Egg 3: Employee Training – Your First Line of Defense

Empowering employees with effective cybersecurity training is pivotal, as they play a dual role as both the strongest and potentially weakest links in your cybersecurity chain. When delving into the essential components of regular cybersecurity training, it's essential to emphasize key areas such as phishing awareness, equipping employees with the skills to recognize and thwart phishing attempts. It's crucial to be vigilant about a common tactic used by attackers – the sense of urgency. Consider this: if your boss has never requested a sudden billing change via email before, it's a red flag if it happens out of the blue. Anything that seems off-brand for the person you're communicating with should raise concern.

Another critical aspect is verification. Safe internet practices should cover the importance of avoiding suspicious links and practicing cautious online behavior to mitigate potential threats. When you receive a link or communication from someone, take an extra step for security. Create a new email, send it to them, and verify the legitimacy of the information. It's an additional layer of protection, ensuring that the communication is genuine. Always ensure that this verification process takes place within the confines of a new email. Replying to the email only goes back to the attacker. A new email allows ensures you send it to the appropriate person and confirm they were the ones who sent it.

To foster an environment where cybersecurity is a shared priority, ongoing conversations are paramount. This involves creating an atmosphere where employees feel comfortable discussing potential threats, sharing insights, and actively participating in cybersecurity initiatives. Leadership plays a pivotal role in setting the tone for this culture, demonstrating a commitment to cybersecurity through consistent communication, support, and proactive engagement. A shared understanding of the importance of cybersecurity creates a collective defense mechanism within the organization.

Incentivizing employees to adhere to best practices is essential for creating a cohesive and proactive approach to cybersecurity within the workplace. Best practices encompass a range of actions, including regular software updates, secure password management, and adherence to company cybersecurity policies. Recognition programs, training incentives, and rewards for exemplary cybersecurity behavior can be powerful motivators. Creating a culture that values and rewards cybersecurity mindfulness establishes a proactive stance, where employees actively contribute to the overall security posture of the organization.

Easter Egg 4: Regular Security Audits

In cybersecurity, we use a zero trust architecture. This principle states, "never trust, always verify." This is a paradigm shift from what we used to do. Instead of assuming access based on roles or device ownership, it's more secure to continually prove device trustworthiness. Implement periodic security audits, with a suggested frequency of quarterly or annually, including penetration testing for a proactive defense. Leverage Threat Intelligence, akin to a SIM, to consolidate logs, enhancing visibility and simplifying analysis. Additionally, prioritize incident response planning and disaster recovery exercises, ensuring preparedness. Consider incorporating recommended tools for each section to fortify your cybersecurity strategy.

Security audits are essential for identifying vulnerabilities in your network and systems. The frequency of your security audits depends on the nature of your business and the sensitivity of the information at stake. For high-security environments, such as those housing government secrets or groundbreaking medical discoveries, a monthly or bi-monthly audit becomes imperative. The key lies in establishing a baseline through thorough penetration tests, recording system changes, and conducting subsequent tests to ensure the efficacy of new control measures. Whether expanding with a new office or implementing policy updates, periodic audits, at least on a yearly basis, coupled with follow-ups, form a proactive approach to fortifying your organization's cybersecurity posture. The frequency of these assessments should align with the evolving needs and vulnerabilities of your specific business landscape, turning the process into a tailored, ongoing strategy for robust defense.

A key tip is to create a security audit schedule. In this schedule, detail the process of establishing a routine for security audits, discuss how often audits should be conducted, who should perform them (internal staff vs. external experts), and the steps involved in responding to the findings of an audit. Running updates is a crucial step. Failure to update systems exposes them to various vulnerabilities, including unpatched security holes, obsolete software risks, and potential unauthorized access. Outdated systems compromise data integrity, invite malware infections, and risk network security. The consequences of neglected updates range from data breaches to service disruptions, emphasizing the critical role of regular updates in safeguarding against evolving cyber threats.

For updates and patches, there are no Easter eggs; it's a straightforward task that needs attention. Regarding advanced endpoint protection, the Easter egg lies in acknowledging the limitations of traditional antivirus software, emphasizing the necessity for newer Endpoint Detection and Response (EDR) solutions. Unlike older systems, modern EDR, like Sentinel One, scans real-time system changes, providing a more proactive defense against evolving threats without relying heavily on definition updates.

If you find yourself uncertain or lack the expertise in conducting these assessments, it's advisable to seek the assistance of cybersecurity experts, like Vertilocity, who can navigate the intricacies of the process with precision and ensure the highest level of protection for your organization.

Easter Egg 5: Navigating Artificial Intelligence (AI)

AI has become a pervasive term, encompassing various forms such as machine intelligence and generative AI. While machine intelligence operates within software, not facing the external world, generative AI, like ChatGPT, accesses learning through the internet. However, it's important to note that ChatGPT doesn't truly learn; it offers estimated guesses, resembling an advanced Google search.

Concerns arise regarding the updating of AI systems. ChatGPT 3.5, for instance, is frozen at a specific point in time. Upgrades prompt transitions to newer versions but don't entail continuous learning. The initial intelligence of AI systems can diminish when exposed to broader, less curated data.

When considering AI's role in security, it's crucial to distinguish between generative AI and closed-circuit machine learning. Generative AI, often open source, may pose security threats. For practical application, leveraging internal versions that enhance automation without compromising security is advisable. Always exercise caution with generative AI. Don’t include personally identifiable information (PPI). A good rule of thumb, if you wouldn’t send it in an email to an external employee, don’t put it in generative AI.

A Basket Full of Cybersecurity

These cybersecurity "Easter Eggs" are not just seasonal but crucial year-round practices. By embracing these strategies, your business can build a robust defense against the ever-evolving threats in the digital world. Now that you have a fuller basket of knowledge, you can be a better safeguard to your business against the slyest of cyber threats during your cybersecurity hunt.

Contact us at MSP@vertilocity.com for more information on cybersecurity defenses and discover what solutions may work best for your organization.