

COMMENTARY



Cybersecurity and Fraud Prevention:

Lessons from recent cyber incidents

In the wake of the recent discussions surrounding the Microsoft CrowdStrike incident, the perception of cybersecurity vulnerabilities has become more pronounced. Even though a cybersecurity breach did not cause this situation, it was caused by a content update for CrowdStrike's Windows sensor which caused a system crash that affected Microsoft and other businesses globally; it underscores the importance of vigilance. When concerns arise around a leading cybersecurity firm like CrowdStrike, it highlights any organization's potential risks. While understanding these situations is essential, it's even more crucial to learn from them and proactively strengthen defenses against possible threats.

Implementing Multifactor Authentication and Tiered Access to Mitigate Ransomware Threats

To safeguard your business effectively, it's crucial to control access to your network. Imagine a scenario where ransomware—malicious software that locks you out of your files, systems, or networks and demands a ransom for their return—manages to infiltrate your defenses. This threat can either create an initial infection or spread rapidly once it gains a foothold. To mitigate such risks, it's essential to ensure that only authorized personnel have access to critical parts of your network. One effective strategy is to implement multifactor authentication

(MFA), which adds an extra layer of security. By requiring multiple forms of verification, MFA makes it significantly harder for unauthorized users to breach your defenses. It's also vital to create a tiered access for users. Only a few employees need access to every system or database. Implementing a tiered-access approach is a best practice. A simple way to do this is to separate accounts and access based on roles, i.e., administrative and non-administrative. This strategy prevents non-administrative accounts from disabling antivirus software or other security measures, allowing your IT team to limit access based on an individual's function, role, or title. No authorization should mean no access. Regularly review, minimum quarterly, and update user permissions to align with current job responsibilities.

Verifying Users Before Password Resets Reduces Fraud Risk

Another crucial step in protection is validating users before resetting passwords. Using one-time tokens, automated processes, and thorough questioning of those requesting password resets can significantly reduce the risk of scammers impersonating employees to gain access to accounts. Always verify the identity of users before allowing any changes to their credentials. Encourage strong, unique passwords and educate employees on



“All organizations must remain vigilant and proactive in their cybersecurity strategies.”

the importance of not reusing passwords across different platforms.

Using Immutable Backups and Antivirus Software to Combat Malware

Antivirus software and endpoint detection can prevent unauthorized applications, such as malware. These tools help detect and neutralize threats before they can cause significant damage. Maintaining immutable backups—written once and not modifiable—also protects against ransomware, malware, and other threats designed to steal data and disrupt your IT network. Regularly update and securely store these backups. Test backups periodically to verify their integrity and reliability.

Conducting security simulations and ongoing training is one of the most effective ways to prevent cyberattacks. Regular training on recognizing and responding to threats, and periodically test your employees to ensure they understand how to respond. An alert and prepared team can catch a surprisingly high percentage of potential threats. Phishing simulations, for example, can help employees identify suspicious emails and avoid clicking on potentially harmful links.

Employee Training and Phishing Simulations: Essential for Cyberattack Prevention

Beyond these technical measures, small businesses should also be aware of social engineering tactics used by cybercriminals. These attacks often start with attempts to create panic and provoke immediate, rash actions. Train your employees to pause and verify the legitimacy of unexpected messages or requests, especially security-related ones. Encourage a culture where employees feel comfortable reporting suspicious activity without fear of reprimand.

Monitor and update your security policies regularly to reflect the latest threats and best practices. Consider implementing a zero-trust security model, which assumes that every attempt to access your systems could be

a potential threat. This model requires continuous verification of user identities and device security status before granting access to resources.

Another critical aspect of cybersecurity is securing your business’s financial transactions. Use secure payment processing methods and monitor your accounts regularly for unauthorized transactions. Implement alerts for large or unusual transactions to catch potential fraud early. Educate your employees about common scams, such as business email compromise (BEC), where attackers pose as company executives to trick employees into transferring funds or sharing sensitive information. Many attacks begin by creating a sense of panic, prompting immediate and often rash actions. If you receive a message about your cybersecurity, pause and take a deep breath before doing anything drastic. The above tips will help you prevent an attack but staying calm and methodical in your response is equally important.

The attention garnered by the Microsoft CrowdStrike incident serves as a powerful reminder of how the perception of cyber threats can impact businesses. Just as Microsoft had to address concerns, all organizations must remain vigilant and proactive in their cybersecurity strategies. Regularly updating defenses and staying informed about emerging threats is vital to safeguarding your business against real and perceived vulnerabilities.

About Kyle Guest

Kyle Guest is the vice president of business services for Mountain America. He joined the credit union in 2021. Guest has been in the financial industry for over 16 years, specializing in commercial relationship management and cash management products. He is passionate about enhancing Mountain America’s business technology offering and strives to improve all business members’ daily banking processes and overall experience with Mountain America Credit Union. Guest resides in South Jordan with his wife, Megan, and their four children.