Educating SMBs About Increased Cyber Risks

by Steve Brown

cybercriminals | cybersecurity | cyber risk

Summary: Cybersecurity is a constant concern. Yet, with the latest Russian cyber threats, it is becoming even more important. Your small business customers could be affected, directly and indirectly. So, we dig deeper to provide you with the current top threats and critical protective measures.

Archaeologists discovered that Ecuador's Mayo-Chinchipe culture ground cacao beans, vanilla, and other spices into a chocolate drink 5.3K Ys ago. But, feeding the craving for chocolate has been far easier since 1847, when British chocolatier JS Fry molded the first chocolate bar. The world's love of chocolate runs long and deep, even when it comes to animals. Yet, for animals such as dogs and cats, this sweet treat can actually be deadly, as they are unable to metabolize the alkaloid theobromine found within cacao beans. Clearly, good things can contain risks at the same time.

Similarly, many small businesses have been able to keep their operations afloat during the pandemic, thanks to technology and the internet. Yet, this increased reliance on interconnected systems has also put them at greater cyber risk. Now, with the warnings about cyberthreats from Russia, small and medium-sized businesses (SMBs) need to be even more vigilant. To minimize the chances of cybercriminals compromising the security of small business customers, community financial institutions (CFIs) should be actively educating this group about what they should watch out for and how to protect themselves.

SMB customers at risk

More than 30% of SMBs are at risk of cyberattacks, according to the cybersecurity firm, CyberCatch. Its January report found that hackers specifically target SMBs, due to the fact that their security measures tend to be less effective than those of larger organizations. Not only that, but with the current Russian cyberthreats, experts say that larger targeted companies could affect smaller businesses that are connected to their platforms.

Top threats

Spoofing, sniffing, and clickjacking are the three biggest cyber risks for SMBs right now. While having anti-malware software in place is a good start, it isn't necessarily enough. Given this reality, it is important for SMBs to know the differences between each of these tactics to be on the lookout for these cyber malfeasances.

- **Spoofing** is when cybercriminals mask their identities using phony IP addresses designed to appear like those of legitimate — usually well-known and recognizable — organizations in order to get the trust of an individual to click on a link or attachment. Once they click on the link or attachment, malware is installed on their device. According to CyberCatch, roughly a third of SMBs have fallen prey to spoofing attacks.
- **Sniffing** is the real-time interception of packets of data that pass through a network in order to capture sensitive information, such as passwords, credit card information, etc. Cyberthieves use programs and devices, known as sniffers, that can monitor everything from an organization or an individual's email and web traffic to router configurations, FTP passwords, and DNS traffic. While

there are legal uses for sniffers, such as FBI wiretaps and monitoring, criminals are looking for any unprotected and unencrypted information that they can exploit. The most common way that people fall victim to sniffing attacks is by using Wi-Fi networks that are unsecured.

- **Clickjacking** is when someone compromises the user interface (UI) on a legitimate website so that someone is clicking on something other than what appears on the screen. By hiding a different UI within or on top of a legitimate site's normal UI, criminals are able to do things, such as install malware on an individual's computer or steal credentials. In some cases, criminals will hide clickjacking so well by mimicking the expected result that an individual has no idea nothing is out of the ordinary. Clickjacking is possible on websites that use HTML frames that enable content to be displayed independently within a separate window.

Protective measures

- **Identify your organization's most valuable data** and information and ensure that it is backed up somewhere separately, should a malware attack occur.
- **Encrypt both outgoing and incoming communication** using a virtual private network (VPN).
- **Conduct internal IT network audits** using device auditing or bandwidth monitoring.
- **Regularly test all systems**, from software to web applications and websites, and look for any anomalies.
- **Patch any security weaknesses** identified immediately.
- **Limit administrator privileges**.
- **Require remote workers to use only secured Wi-Fi networks**, particularly when working with sensitive customer data. Cybercriminals sometimes create phony public Wi-Fi connections that are unsecured, hoping that unsuspecting people will utilize them.
- **Employ ethical hacker**s to help identify any weaknesses within your security measures.
- **Maintain a recovery plan**, if and when a cyber threat happens. This would include firming up entry points, changing system passwords, and accessing data from another location, among others.

Cyber risks are ongoing, yet now there are new threats arising. So keep your SMBs safe by communicating the largest threats, along with ways they can protect themselves. This will help mitigate these rising threats.