Train your members to be cyber smart

September 28, 2022by **MICHAEL SEIDELMAN**, **THINK|STACK**

Cybersecurity has been a top concern for businesses for the past year as the number and impact of cyber attacks has increased drastically.

According to an article from Business Insider, reports have shown that “63% of financial institutions experienced an increase in destructive attacks, an increase of 17% from last year.”

While leaders are focused on improving cyber protection and strategies to prevent attacks and mitigate risk, consumers are not always as aware or concerned about how certain behaviors could expose them to risk.

As reported by SCMedia, FICO's recent 2022 Digital Consumer Banking and Fraud Survey found that financial customers are "too complacent about the risk certain fraudsters pose, with only 5% worrying about real-time payments fraud, and many unwilling to accept new fraud management measures."

Despite the growing cyberthreats, nearly three-quarters (72%) of U.S. financial customers believe "their banks do enough to keep their money safe".

However, nearly half (46%) of U.S. financial customers who took part in the FICO study claim to have been victims of fraud and "nearly one in five (19%) have suffered account takeover fraud scams."

Regardless of the level of concerns of customers, financial institutions, including credit unions, must develop, monitor and evolve risk management strategies to reduce threats to members and their data.

SCMedia quotes Nikhil Behl, chief marketing officer at FICO, "Even if consumers are not overly worried, financial institutions still need to be on their behalf. Organizations will need to continue to adapt and evolve to fight existing and emerging fraud threats. At the same time, they need to carefully balance fraud management with sustaining customer trust, and delivering frictionless digital and in-person customer experiences."

With the increase in access and use of digital banking and digital currency, credit unions need to have more heightened awareness of potential cyber threats and ways to protect members as the cyber attack surfaces grow.

In an article from SCMedia, Assaf Keren, vice president of enterprise security at PayPal, shares, "If the pandemic taught us anything, it's that we're in an inflection point for digital currency and digital experiences across the board. People don't want to handle cash anymore. And I think that digital wallets, digital currencies and blockchain technology or blockchain-based currencies are the future."

According to the FICO study, nearly 3 in 10 U.S. consumers say they would change banks if they feel their fraud incident was poorly dealt with.

Cyber threats are not a lost cause, and the risk can be mitigated with the right partners and training. Human error is to blame for a majority of attacks and with more customers using online banking and more employees working remotely, training and new policies are needed.

So, what can credit unions do?

- **Develop an awareness campaign:** Educate customers about cyber attacks and ways to mitigate risk. Using email, branch signage, text messages and social media, provide customers with insights and tips that are easy to understand and use. Frequent messaging will be important to reinforcing the importance of awareness and prevention.
- **Host/sponsor events:** Leverage exhibition tables and speaking engagements to share critical information and education materials with the public regardless if they are customers.
- **Train employees:** In addition to training employees for ways to identify and mitigate cyber attacks, provide them with simple talking points and educational materials to share with customers.

Contact us to learn more about our cybersecurity services and training for credit unions.

Michael Seidelman

Michael Seidelman is Director of Cybersecurity for Think|Stack, a Managed IT Services CUSO specializing in cloud and cybersecurity solutions for credit unions and non-profits. He can be reached at ...DETAILS