Social Media Risks For Banks

cyber security regulatory risk management

Summary: Social media financial scams reached $420mm for the top 25 largest US banks. Tactics for banks to manage social media risk and still stayed connected socially.

Pew Research finds that 1Y ago some 69% of Americans said they were using at least one social media site. This number is most likely larger today and it is interesting that retiring boomers are driving a chunk of this growth. Most people cannot imagine getting through their day without taking a minute to read their friends' Facebook posts, tweet about a life or news event, or post a selfie on Instagram. This said, online "socializing" for bank employees and customers does have its risks.

In the wake of the social media revolution, where literally billions of people around the world share their photos, schedule, location, and often their most personal and sensitive information, cyber-criminals have become increasingly savvy too. These bad actors now target people and businesses directly using their social media presence.

Such social media cyber-attacks can take many forms. These include sending out malware through a social site messaging application, to generally over-loading a bank's own social media page. Bumping it up a notch, bad actors also offer bogus services or use botnets to collect personal details on a broad scale to either sell the information directly, or use it to break into data stores, payment systems or other more lucrative targets.

In 2015, the Pony botnet stole more than 2mm passwords from users on Facebook and other social media sites. More than one in five social media users (22%) say they have fallen prey to some kind of security incident on a social site, according to research from Stratecast. Facebook even admits there is fraud afoot, recently confirming publicly that as many as 100mm of the site's active user accounts could be fraudulent or fake.

In 2016, the cost of social media financial scams reached $420mm for the top 25 largest US banks alone, according to research from cybersecurity firm ZeroFox. It also found that three such financial scams are created for each one that is found and taken down. One of the social networks that ZeroFox investigated had nearly 250k fraudulent posts for one type of scam.

While preventing employees and customers from visiting social media sites may be impractical, there are tactics to manage your social media risk.

Start by making everyone aware of the potential compliance concerns here. Banking is nothing if not regulated. When it comes to social media, the rules can change from year to year or month to month.

Next, make sure your compliance and human resources departments are plugged-in with up-to-date information on what is and is not permissible to share about the bank, its customers, or even one's self, as an employee of the bank. The same goes for rules about when and where social media access is permitted, as part of the bank's own policy.

Third, closely follow your bank's own social media reputation. Chances are that someone out there is talking about your bank. While it's not important to track every mention, there should be at least one point person who is responsible for regularly combing the bank's own social media posts, pages and comments for suspicious or fraudulent activity.

Finally, educate employees about the risks. Make sure all employees, including executives and board members, are aware that even a casual reference to being on vacation, or naming their childhood pet, could be opening the door to hackers who are seeking just this kind of personal information. As part of consistent cybersecurity training, reinforce that malware can come through this channel as easily as through email.

CECL SOLUTION - BUILT BY OUR BANK FOR YOUR BANK

CECL is one of the biggest challenges for community bankers these days. Our experts are ready to guide you every step of the way through this integration with no software to maintain. Learn more about our CECL Solution.