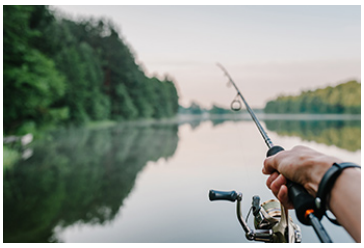

Business Email Fraud Is Growing

cyber security risk management

Summary: Cybercriminals are bold these days, as cyberattacks remain lucrative for them. In 2020, more than 19K businesses and individuals lost over $1.8B through email fraud, more than any other type of cybercrime. The best defenses for financial institutions in the fight against business email compromise are employee training, KYC & suspicious activity tracking along with security tools and customer information.

You may not know this, but today is National Go Fishing Day. Going fishing sure sounds appealing, as summer sets in. Yet, with all the cybercriminals doing their own phishing, you may not want to take the day off just yet.

Cyber thieves are getting bolder every day , as we highlighted yesterday. While much attention recently has focused on ransomware attacks, including the one that shut down an east coast oil pipeline company, Business Email Compromise (BEC) and Email Account Compromise (EAC) fraud remains one of the most common scams affecting business and individual bank accounts. According to the FBI's Internet Crime Report for 2020, more than 19K businesses and individuals lost over $1.8B through BEC/EAC fraud scams, more than 3x the amount of the next leading type of cybercrime.

A case in point. An example of how a BEC scam happened to a smaller branch of a financial institution (FI) in TX underscores the seriousness of this issue and provides more warning signs for all FIs, including community financial institutions (CFIs).

First, the hacker broke into the email of a bookkeeper at a non-profit organization in San Francisco. The organization had $650K in grant money intended for a housing project for the poor, which was criminally redirected to a bank account at an FI branch in TX. This FI is one of the largest and oldest in the state and has over 50 branches just in the San Antonio area. But this all happened 350 miles away from San Antonio in a town with a population of just over 100K in a branch with more of a CFI feel.

Apparently, a straw customer (also called a mule) working with the fraudsters opened an account in the branch to receive the stolen money. The scammer then used convincing emails to inform the bookkeeper in San Francisco that the regular bank for the grant money was undergoing an audit and so the funds should be transferred instead to the account at the TX branch. The bookkeeper helpfully wired the money in three installments. Once the money arrived, it was swiftly withdrawn by the scammer. As of yet, the funds have not been recovered (except for a small amount left for the mule) and the case remains unsolved.

Email fraud doesn't always involve an FI. But when it does, the institution needs to have strong defenses to help prevent its own funds from being stolen or from being used as a vehicle for an email scam against someone else.

The best defenses

Employee training. The most effective protection is thorough and ongoing training of employees who are on the frontlines of the war against email scams. Providing videos or even enlisting a third party for drills are just a couple of ways to keep your employees updated on the latest versions of this ongoing fraud.

KYC and suspicious activity tracking. It is also imperative that CFIs make sure all employees understand and follow the protocols for opening accounts, identifying customers, and handling unusual or large transactions. Know-your-customer techniques are critical in flagging suspicious account activity. Internal processes flagging suspicious activity should be easy-to-follow and effective at protecting. Artificial intelligence (AI) programs can help track and flag suspicious activity too.

Security tools. Security tools like two-party authentication should be employed as another security layer to confirm identities. Make sure that security software is updated regularly for these to work properly.

Customer information. Your customers should also receive vital important about these email scams. You could dedicate a page of your website to BEC and how to stay safe. Or you could send regular email reminders. These are just a couple of ways to do this.

Email scammers around the globe are constantly probing for weak links in business operations. A CFI can present a tantalizing target for these scammers looking for a quick way to deposit and then quickly withdraw fraudulently obtained funds. Hopefully, this example reminds us all to keep our guard up at all times to stop these cyberthieves in their tracks.

STRESS TESTING: TOP-DOWN OR BOTTOM-UP

In this market, it is important to stress test your loan portfolio. We offer multiple approaches that will fit your needs and your regulatory compliance requirements. Quickly stress test your loan portfolio and get pre-exam assistance. Learn more about stress testing today.

ECONOMY & RATES

Rates As Of: 06/18/2021 05:38AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.04	0.03	-0.05
6M	0.06	0.03	-0.03
1Y	0.08	0.03	-0.03
2Y	0.25	0.10	0.12
5Y	0.90	0.11	0.55
10Y	1.51	-0.08	0.60
30Y	2.10	-0.18	0.46
FF Market	**FF Disc**		**IORB**
0.06	0.25		0.15
SOFR	**Prime**		**OBFR**
0.05	3.25		0.04