Helping Your Customers Combat Online Crime

cyber security ransomware phishing

Summary: Online crime has increased during the pandemic, unfortunately. The latest FBI internet crime report shows that 241K victims have fallen prey to phishing or related scams, business email compromise has resulted in losses of greater than $1.8B, credit card fraud claimed almost $130MM in losses, and 2.5K ransomware complaints were filed. We give you reminders to continue to stay safe along with your customers.

Agatha Christie wrote, “Murder on the Orient Express,” which is considered to be one of her best works, in 1933. The Belgian detective Hercule Poirot sure had it easy compared to searching for online criminals today.

Online crime has surged during the pandemic, as the FBI’s Internet Crime Complaint Center (IC3) received a record number of complaints in 2020 and more than $4.2B in losses reported by victims to US authorities.

Already banking regulators have cracked down and cyber scrutiny is high, with more likely to come. Just recently, Congresswoman Maxine Waters, Chairwoman of the House Financial Services Committee, sent a letter to senior members of the House Committee on Appropriations, Subcommittee on Financial Services and General Government, urging them to support supplemental funding to the Financial Crimes Enforcement Network (FinCEN).

Heightened attention to these matters means bankers need to stay informed and continue passing on critical safety information to customers. Accordingly, we offer you some highlights from the FBI’s latest report that you may find particularly relevant.

Phishing and related scams

Not surprisingly, phishing/vishing/smishing and pharming, all variations of scams involving the usurping of personal information, had by far the most victims in 2020, topping out at over 241K. Community financial institutions (CFIs) should continue to warn customers about what each of these is and the dangers posed. In short,

- ***Phishing*** refers to scam artists trying to elicit personal information, usually through email.
- ***Vishing*** relies on social engineering to trick you into providing information via phone so fraudsters can access your personal accounts.
- ***Smishing*** uses cell phone text messages to lure unsuspecting customers
- ***Pharming*** is a scam where hackers install malicious code on a personal computer or server, which redirects you to a fraudulent Web site without your consent or knowledge.

Business email compromise

Not new, but still another area of concern to CFIs is business email compromise (BEC). In 2020, the IC3 received over 19K of these types of complaints with adjusted losses of more than $1.8B. As a refresher, to affect this type of scam, thieves use legitimate business email accounts to pose as the CEO or another executive and request the transfer of money.

These attacks have become more sophisticated over the years, and now include the compromise of personal emails, vendor emails, lawyer email accounts, requests for W-2 information, and fraudulent requests for large amounts of gift cards.

Credit card fraud

It should go without saying that this should be an area of concern for financial institutions. Last year, there were over 17.5K victims of credit card fraud, up from just over 14K in 2019 and around 15K in 2018, according to the report. That translates into $129.8MM in 2020 vs. $111.5MM in 2019 and $88.99MM in 2018. With the boost of e-commerce these days, credit cards have been used more frequently online and can easily be lifted unsuspectingly too.

Ransomware

This cybercrime is especially troublesome since many businesses have been hit hard by the pandemic and can't afford to lose any data to fraudsters. In 2020, the IC3 received almost 2.5K complaints identified as ransomware with adjusted losses of over $29.1MM. Though it can be tempting, CFIs should be aware and remind their customers that the FBI discourages paying ransom to cyber-thieves. Authorities are concerned that paying will encourage additional criminal behavior and it doesn't guarantee recovery of the victim's files.

Ways to stay safe

There are many ways for you and your customers to stay safe.

1. Always back up data to an offline source, such as an offsite server.
2. Make sure that multifactor authentication is used whenever possible to ensure that customers are truly who they say they are.
3. Geolocation can also help in stemming credit card fraud, since you are able to find out where the cardholder is (and is not).
4. Keep training your employees and communicating with your customers. This should be a regular occurrence.

We hope your customers don't fall prey to any of these scams. But if they do, making sure your institution understands the latest dangers and the steps they should take to quickly mitigate the problem can make a world of difference in keeping their information and assets safe and secure.

PCBB INTEGRATES WITH FISERV WIREXCHANGE: FX

PCBB integrates with Fiserv's WireXchange®: FX platform and offers access to our sophisticated international wire services. With PCBB, Fiserv customers will also get access to innovative enhancements such as SWIFT gpi payments and tracking. Learn more about our Fiserv WireXchange integration.

ECONOMY & RATES

Rates As Of: 04/29/2021 04:15AM (GMT-0800)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.01	-0.02	-0.08
6M	0.04	-0.01	-0.05
1Y	0.05	-0.01	-0.05
2Y	0.17	0.01	0.05

5Y	0.89	-0.06	0.52
10Y	1.67	-0.08	0.75
30Y	2.33	-0.08	0.68
FF Market		**FF Disc**	**IORB**
0.07		0.25	0.10
SOFR		**Prime**	**OBFR**
0.01		3.25	0.06