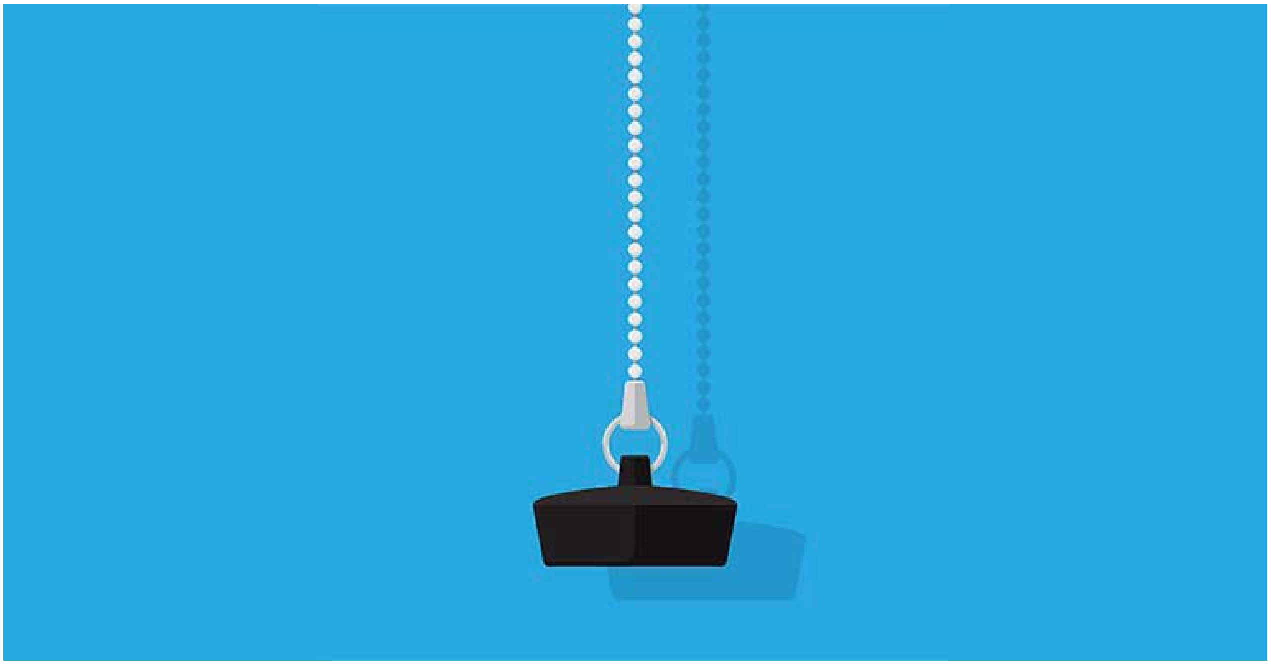
Uncertainty is fueling fraud. Here's how to stop it

March 1, 2021



Recent data shows that the pandemic has allowed fraud to grow. Cybersecurity experts share ways for community banks to prevent potential attacks, as well as information to pass onto customers to arm them with fraud prevention strategies.

By Katie Kuehner-Hebert

The COVID-19 pandemic has wreaked havoc in so many ways, including spurring new cyber threats involving fraudsters preying upon the disruption and uncertainty.

Within the first quarter of 2020 alone, digital attack rates were 20% higher than in the prior quarter, and payment attacks were 49% higher than they were at the end of 2019, according to Arkose Labs.

> "If this pandemic has given fraudsters anything, it's the chaos and uncertainty they need to be successful."
> —Steven Estep, ICBA

“If this pandemic has given fraudsters anything, it’s the chaos and uncertainty they need to be successful,” says Steven Estep, ICBA’s assistant vice president of operational risk.

Much of the fraud occurring during this time involves social engineering, which is when a criminal poses as someone else to trick customers into divulging banking credentials or conducting fraudulent transactions.

Fraudsters are taking advantage of the fact that many people have gone through changes to their everyday routines, such as moving to remote work or losing their jobs due to the pandemic, Estep says.

“Understandably, it’s been a lot easier for people to click on links in a phishing email,” he says. “They may have been caught offguard just because of the uncertainty or because of the desperate times they may be in.”

In fact, many phishing attacks are aimed at getting people to click on links related to the pandemic, according to Jeff Olejnik, principal, CyberTech practice leader at Wipfli LLP in Minneapolis.

“For example, one email circulating [tells] the recipient that they’ve been identified as someone who may have been exposed to another person who contracted COVID-19,” Olejnik says. “The email provides a link for the person to validate they’ve received the alert, but in reality the link enables the fraudster to download malware onto the recipient’s computer.”

Quick stat

20%

The increase in the rate of digital attacks between Q1 and Q2 2020

Source: Arkose Labs Q2 2020 Fraud Report

> “Many companies quickly put in some of the cloud services and communication platforms as people started working from home, but they didn’t turn on the security features like multifactor authentication and restricting who has access.”
>
> —Jeff Olejnik, Wipfli LLP

Attacking bank or work systems

Another tactic is when a fraudster impersonates someone from the company, such as a human resources director, asking the recipient to confirm their employee benefits selection, Olejnik says. But in reality, the phishing email is aimed at gaining the recipient’s username and password to log into the company’s VPN (virtual private network) or Office 365, assuming the company doesn’t require multi-factor authentication. (Multifactor authentication is when an employee needs more information than just a username and password to log in, such as a one-time passcode that is texted to their device.)

Fraudsters are also attacking communication and collaboration cloud services, such as Microsoft's Dynamic 365 or Teams, which many companies deployed as the pandemic threat increased.

"When the shutdown first happened in March, many companies quickly put in some of the cloud services and communication platforms as people started working from home, but they didn't turn on the security features like multifactor authentication and restricting who has access," Olejnik says. "So, hackers are exploiting this, as well as workers' weak passwords, such as the popular 'Winter2020!'"

Robert Johnston, CEO of Adlumin, a cybersecurity and compliance software provider based in Washington, D.C., says fraudsters who are able to log into a bank's network could also gain access to an employee's credentials. That means they could access the bank's teller, loan origination, customer relationship management (CRM) and other systems.

"Bank employees should not use simple authentication," Johnston says, "which in most cases is actually a [regulatory] violation … Instead, use multifactor authentication."

Fraudsters have taken advantage of new information-gathering avenues made possible by the pandemic, such as the flood of unemployment claims and stimulus payments. This creates opportunities for fraud and cybercrimes, according to Teresa Walsh, global head of intelligence at Financial Services Information Sharing and Analysis Center (FS-ISAC), who is based in London.

"Fraudsters are using the same social engineering techniques they have always used to trick people into clicking and/or allowing access to accounts, such as phishing, smishing and business email compromise," Walsh says. (Smishing, a portmanteau of "SMS," otherwise known as texting, is a form of phishing via texts instead of emails.) "The difference [now] is they have been exploiting the urgency and fear around COVID-19 as a lure, and, unfortunately, it is a powerful lure."

Expert cybersecurity advice

Community banks should take an active role in helping their customers avoid hacking attempts. Teresa Walsh, global head of intelligence at FS-ISAC, says community banks should:

- Regularly educate and train employees to maintain situational awareness and report any potential issues immediately. Provide real-world examples and repercussions of successful frauds.
- Perform regular tests to assess employees' knowledge and ability to recognize and prevent fraud.
- Participate in cybersecurity organizations' information sharing to get advanced knowledge on the motivations and tactics behind new fraud methods.
- Implement multifactor authentication for their employees and their customers.

Phishing and smishing

Sometimes the evidence of a successful phishing attack is immediate, and other times bad actors implant malicious code to monitor, survey and exploit someone at a later date, says Wade H. Barnes, financial services practice leader at Hartman Executive Advisors, an independent strategic technology and cyber advisory firm based in Timonium, Md.

“Phishing attacks remain one of the single most impactful threats,” he says, “as it only takes one employee to click a link or download an attachment [to] cause great harm within the organization despite all of the protections IT has in place.”

10 cybersecurity tips to share with customers

ICBA recommends that community banks advise customers to:

1. **Enable the strongest authentication tools** offered by their bank. Popular authentication methods include biometrics, security keys and single-use codes.
2. **Use unique passphrases as passwords** and differentiate them across multiple platforms. Length trumps complexity. A strong passphrase is at least 12 characters long.
3. **Do a system check.** Purge unused apps and outdated or sensitive information stored in old files and emails and ensure all software on internet-connected devices is current.
4. **Manage social media settings and minimize information sharing.** Just a few data points can create a pathway for exploitation by cybercriminals.
5. **Use Wi-Fi judiciously.** Limit the type of business conducted over open public Wi-Fi connections, including logging in to key accounts like banking.

6. **Monitor account activity regularly** for irregular transactions, and report discrepancies to your financial institution immediately.
7. **Back up intellectual property** and other digital information and store it safely so in the unfortunate event of a ransomware or other cyberattack you have a way to retrieve the data.
8. **Read the fine print** when purchasing items online. If prompted, do not save credit and debit card information on the merchant's website or app.
9. **Be mindful when shopping online** and look for signs of illegitimate websites. Spelling or grammatical errors, missing contact information, and suspicious URLs or email addresses are all red flags.
10. **Look for special indicators** such as web addresses with https:// that denote extra measures taken to help secure your information. URLs that end in .BANK are assigned for exclusive use by financial institutions.

Katie Kuehner-Hebert is a writer in California.