Criminals Have A Plan To Steal Your Money. What's Your Plan To Keep It?

Cyber criminals have become more sophisticated than ever. They have multiple plans to steal your money any way they can get it. Thwarting cyber thieves begins with awareness and education – for you and everyone in your organization. Keith Parsons, BOK Financial's Director of Financial Crimes, has some tips that every executive needs to know.

Common Scams and Ways to Defeat Them

1. "Our bank account was compromised…please wire your payments here, instead." A trusted vendor sends an email with new wire instructions, claiming that their bank account was compromised. You wire payment, only to find later the email was fraudulent – and the money is gone. **Prevention tip:** Always verify changes in payment instructions via telephone or in person, and talk to a trusted person you know. "Thieves are watching and listening," Parsons said. "They may hack someone's email and lurk for months, studying how they sound in their emails and who they talk to. They are experts at making an email sound as if it's coming from someone you know."

2. "The boss is on vacation and needs my help!" "Hackers are looking for opportunities, and they can be very patient," Parsons said. "They can figure out your vacation schedule by lurking for months in the background, reading your personal email, or even following you in the news or on social media. When you're out of the office and perhaps unreachable by phone, they strike. An employee receives an email from the boss's personal email account, requesting an emergency wire payment to a key supplier. The employee wires the funds – only to learn later the request was fraudulent. **Prevention tip:** Tell employees you will * NEVER * communicate payment instructions via personal email – and stick to it!

3. "Let us prove we can save you money." Every business owner wants the best deal possible, especially on overhead expenses like office cleaning services. A recent scam uncovered thieves posing as a cleaning crew to offer their services for just one night at a cut-rate price to prove what they could do. "All they prove is that they can steal," Parsons said of one group of thieves recently arrested while working their way across the U.S. "They get access to your offices, but they don't clean a thing. Instead, they spend the night rummaging through desks and file cabinets, looking for checks, check stock and bank account numbers. They cash counterfeit checks and are on to the next unsuspecting victim." **Prevention tip:** "It sounds like a cliché," Parsons said, "But if something sounds too good to be true, it probably is. Do business with people you know. Secure checks and bank statements just as you would cash."

4. "We just don't have the staff to require two people to authorize a wire payment." This is a common dilemma, especially since automated systems have led to more thinly staffed accounting operations. "Criminals know your pain," Parsons said. "They're counting on it." Thieves use multiple schemes – telephone, email, text messaging, etc. -- to steal computer credentials of the employee in your organization who can authorize wire transfers. **Prevention tip:** "The best thing you can do to make it harder for them is to have two people approve every wire, every time," Parsons said. "It takes a little more time, but it is the absolute best way to fight wire fraud."

5. "Technology to fight fraud is too expensive." "Criminals make more than $5 billion off of fraud every day," Parsons said. "They perfect their techniques in foreign countries, then move to the Midwest where they believe banks and their business clients will have fewer checks and balances, and at smaller organizations, less sophisticated technology. **Prevention tip:** Every organization can download free software from IBM, called Trusteer Rapport. "Lots of us have virus software on our computers," Parsons said. "That is important – but Trusteer is also critical to specifically help guard against financial attacks that come in forms other than computer viruses."

Keith Parsons is a Senior Vice President and Director of Financial Crimes at BOK Financial. Before entering the banking industry, Keith worked for the National Security Administration as an Intelligence Analyst and in Counter Narcotics as a Senior Intelligence Analyst.

BOK FINANCIAL®
LONG LIVE YOUR MONEY.℠

Bank of Albuquerque | Bank of Arizona | Bank of Arkansas | Bank of Oklahoma | Bank of Texas
Colorado State Bank and Trust | Mobank