STERLING NATIONAL BANK

Low-tech Fraud Can be High Cost:

HOW TO PROTECT YOUR NOT-FOR-PROFIT FROM CYBER CRIME

Cyber fraud comes in seemingly infinite shapes and sizes, and it is always evolving. Yet despite the shocking scope of the latest data breach or some bizarre new criminal twist that dominates the headlines, companies and nonprofits still have a lot to fear from low-tech cyber fraud.

John J. Murphy
Senior Vice President
Team Leader
Commercial Banking

Patty Marlow
Senior Vice President
Commercial Banking

As part of a commercial banking team that has extensive experience working with not-for-profit organizations, we see frequent attacks and losses from low-tech cyber fraud. That doesn't mean large-scale hacking is not a threat. In fact, some of the fraudulent activity we see day-to-day is done by criminals using stolen information that might have come from one of those significant data breaches that dominate the news cycle. More often than not, however, the actual criminal attempt—sometimes successful—to steal or commit fraud uses social engineering techniques to trick people into making an unauthorized funds transfer.

We want to outline some of the best practices we recommend to our not-for-profit clients to protect against computer-mediated fraud attempts.

Social Engineering and Wire Fraud

Most of the cybersecurity breakdowns we see are social engineering attacks via email. Hackers gaining entry into an online system and diverting funds used to be a more significant threat, but improvements in security have made that harder for criminals to pull off. Social engineering manipulates people into disclosing confidential information or releasing funds inappropriately. If criminals can do that, they don't need to hack into well-protected computer systems. Think of social engineering as "people hacking."

Social engineering attacks often use two techniques, known as "phishing" and "spear phishing."

- Phishing uses fraudulent emails sent to many targets at one time to trick recipients into providing personal information or sending funds to an unauthorized recipient.

- Spear phishing targets individuals—usually managers or executives in financial institutions, companies, or nonprofits—using information gathered about the targets to increase the attack's chance of success.

Sterling National Bank has the resources to help educate your staff about how to protect your organization from account fraud.

Old Fashioned Check Fraud

Don't assume that financial attacks can only arrive by computer. Paper checks may be—theoretically—replaceable by digital transactions, but many companies and not-for-profits still write a lot of checks. It may not be high tech, but check fraud is on the rise. Check fraud can include using counterfeit checks created digitally, forging checks using stolen blank checks, and altering or forging endorsement on legitimate checks.

WHAT TO LOOK FOR. These are some common signs of possible check fraud:

- Different check stock
- Check numbers that are out of sequence
- Inconsistent handwriting or signature
- Checks that are not printed with the client's name
- Purpose or payee that is inconsistent with the client's usual activity
- Indications that a check has been dampened or washed
- A sudden increase in check activity

How to protect yourself. Be alert for signs of fraud, question anything that feels unusual or suspicious, and follow these best practices at all times:

- Avoid mailing checks, especially using outdoor mailboxes.
- Write checks using black gel pens, whose ink is harder to remove or alter.
- Limit access to checks and keep check stock locked up.
- Do not "pre-sign" blank checks.
- Use fraud detection tools available from your bank.
- Review your account activity frequently and question anything unusual.

These techniques often use email to impersonate someone who might legitimately ask the recipient to transfer funds through the banking system. For example, a nonprofit employee might receive an email, supposedly from a client or donor, requesting a wire transfer to a vendor. Or, a bank employee might receive an email, supposedly from a nonprofit, requesting the same type of transfer. If the recipient takes the bait and initiates a wire transfer, the funds actually go to the criminal.

WHAT TO LOOK FOR. Fraudulent email requests often have telltale signs, such as:

- Changes in previous instructions
- Statements of urgency
- A sender who is unable to be contacted
- Unlikely email address
- Contact phone number or email that is not usually used by the sender
- Language that includes errors or is not in the sender's typical tone or style
- Evidence of cutting and pasting, such as different font sizes, grammar shifts, or repetition

HOW TO PROTECT YOURSELF. As bank employees, we receive regular training on how to detect potential fraud, and we share these best practices with our nonprofit clients. Here are some best practices to follow every day, but especially when indications of possible fraud are seen:

- **Be alert to anything out of the ordinary.** If something feels suspicious, trust your instincts and question it.
- **Verify the request by phone using a trusted number.**
- **Know the sender: Does the request make sense?** Is it consistent with the sender's typical operations?
- **Research the recipients to be sure they make sense.**

Best Practices Against Account Fraud

In addition to taking steps to detect and respond to fraud attempts, here are some best practices we recommend to help protect against cyber fraud entirely.

HAVE ROBUST IT SYSTEMS AND STAFF EDUCATION. Whether in-house or outsourced, the IT function must ensure that your systems are protected. This means making sure that virus protection is up to date and that the person in charge takes the threat of cybercrime seriously. However, as you can tell from the discussion of wire fraud, some vulnerability comes from people, not

Review your account activity frequently online, and question anything that seems unusual or suspicious. When in doubt, call your relationship manager.

technology. Your IT function must include ongoing staff education about computer safety, including basics like not clicking on unfamiliar or unexpected attachments and never sharing passwords. These fundamental cyber safety guidelines might be familiar to most people who work in offices, but they are violated frequently, often with disastrous results.

USE SECURE EMAIL. A secure email system encrypts emails as they are sent and received, and requires the receiver to provide authentication. The process can be annoying, but it adds an essential level of security to confidential communications. Sterling uses secure email when we send financial information, and we recommend that our clients do the same. If that's not possible, at a minimum you should truncate any account numbers that you include in email correspondence, showing only a few digits of the entire number. It's also important to be consistent in how you truncate. If you send the first few digits in one email, and the last few digits in another, a hacker who has access to your email account could easily figure out the entire number.

REVIEW ACCOUNTS FREQUENTLY. This is one of the most common ways fraudulent account activity is detected. Use online banking to review your account regularly, and bring any questionable transaction to the bank's attention as soon as you see it. If a fraudulent transaction occurs, the sooner you alert the bank, the higher the chance of recovering the money. If 60 days pass before fraud is detected, it's probably too late. If you find a problem, don't report it once and then let down your guard. Once an account number has been compromised, there probably will be multiple attempts to move money out of the account. So early detection can also prevent additional losses.

USE TREASURY MANAGEMENT TOOLS. Treasury management is how companies and nonprofits keep track of the money flowing in and out of their accounts. Every organization needs to have a good handle on treasury management to be successful. Just as cybercrime has evolved, so have treasury management tools. What started as a relatively straightforward process, such as matching check numbers and check amounts, has evolved into a suite of tools that encompass robust fraud protection.

Key treasury management tools include:

- Courier service to bring checks to the bank
- Online initiation of ACH and wire transfers
- Lockbox services, which are centralized physical or electronic payment destinations that shift payment processing to the bank
- Account reconciliation tools that streamline the process
- Fraud detection tools that identify fraud before checks are paid

There are fees for some of these solutions, but the costs should be weighed against the cost of having to shut down accounts that have been compromised. We advise not-for-profits to have a conversation with their banking team about how these tools work and where they fit into fraud prevention plans.

Sterling National Bank can work with your not-for-profit to help protect against fraud. Contact your relationship manager or Client Services at (855) 274-2800.