PROTECT YOUR BUSINESS
FROM ELECTRONIC FRAUD

A few precautions can make the difference

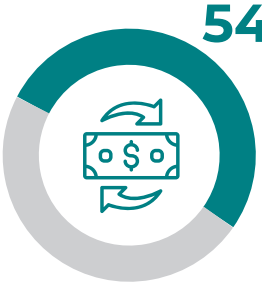
Sony. Home Depot. Target.

These high-profile companies are well known as victims of data hacking throughout the past few years, but businesses of all types and sizes are vulnerable to fraud involving information, wire transfers and other types of payments.

77%

Organizations that experienced payment fraud related to Business Email Compromise (BEC) scams.

54%



Wires are the most common payment method of BEC scams.

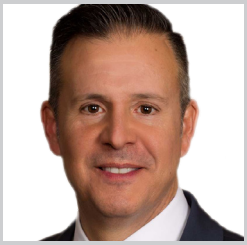
34%

BEC check scams account for another common payment method.

2018 Payments Fraud and Control Survey by the Association for Financial Professionals

Many business owners are aware of the risk of identity theft and take appropriate precautions, but they sometimes don't think about the need to protect their business' banking operations. It's important to have controls in place for your banking accounts because some of the most successful ways to steal money can involve something as simple as the hacking of an employee's email. In a typical scenario, hackers gain access to the email account of a CEO, CFO or other key executive and send an email to a comptroller or another accounting employee indicating that there is an urgent wire that needs to be sent to a specific account. Because the email appears to be authentic and from the executive, wire transfers frequently are completed before fraud is detected.

This type of electronic wire or payment fraud is called spear phishing, which targets high profile executives or employees with malware. But there are other common methods used in electronic payments



Kenneth Romero
Sr. Treasury Management Banking Officer, SVP
New Mexico Bank & Trust
505.946.2502

Jon Parshall
Treasury Management Banking Officer
New Mexico Bank & Trust
505.830.8167

Melissa Tvedt
Treasury Management Banking Officer
New Mexico Bank & Trust
505.830.8171

A typical business or organization loses

5%

of revenue each year to fraud, with a median loss of

$145,000.

Smaller businesses are more vulnerable and suffer disproportionally larger losses, and the median discovery time to detect fraud was

18 months

after it began.

2014 Global Fraud Study by the Association of Certified Fraud Examiners

fraud such as phishing, in which emails are used in an attempt to gain access to sensitive or confidential information, and vishing, in which an automated phone call directs the recipient to contact his or her bank immediately.

Can you guard against hacking?

There is no absolute guarantee you can prevent hacking, but here are some recommendations to help keep your business less vulnerable:

Accept that it can happen to you—It might seem odd, but many business owners do not believe their operations could be hacked, despite numerous high profile examples. Remember that small businesses have been found to be more vulnerable than large operations. One recent analysis found that the U.S. accounts for more than 50 percent of credit card fraud worldwide, but has only 25 percent of total transactions.

Optimize passwords—Don't reuse passwords and don't trust any website to store them securely. To maximize security, set up a two-step process to verify and approve actions and activity for all your online business accounts. Implement password protection and "time out" functions, which require re-login after a period of inactivity, and require strong passwords that must be changed on a regular basis.

Use encryption—Mandate encryption of all data and consider encrypting email within your company if personal information is transmitted. Avoid using Wi-Fi networks because they can allow data to be intercepted.

Don't mix social media with financials—Use separate devices for financial activity, including online banking, email or social media. Keeping those activities separate will reduce the risk that an infected social media website could compromise your banking and business operations.

Secure your computers, systems and data—Make sure you stay current with the latest version of your browser and test its configuration for weakness. Update all operating systems, which have the security improvements embedded in them, and make sure your internet router is secure so the data can't be intercepted.

Enlist your employees' help—Establish a written policy about data security and let them know what types of information are sensitive or confidential and what their responsibilities are to protect that data.

If you have questions regarding additional steps you can take to protect your business from fraud, contact us today.

Tips for preventing wire fraud

- Utilize a dual control process for money movement.
- Never send money from your account solely based on an electronic request.
- Block pop-ups and plug-ins on computers used to conduct business.
- Use separate email addresses for personal/company business.
- Log out of online sessions when not in use.
- Always type the bank's web address into your internet browser rather than cutting and pasting from a link.
- Never provide sensitive information over the phone unless you placed the call or are sure you are talking to the correct party.
- Report suspicious transactions or activity immediately.
- Although hacking and wire fraud are widespread, they are not inevitable and your bank's treasury management team can help you put fraud-prevention measures in place.

Being aware and taking precautions can help ensure your business, your assets and your information stay secure.