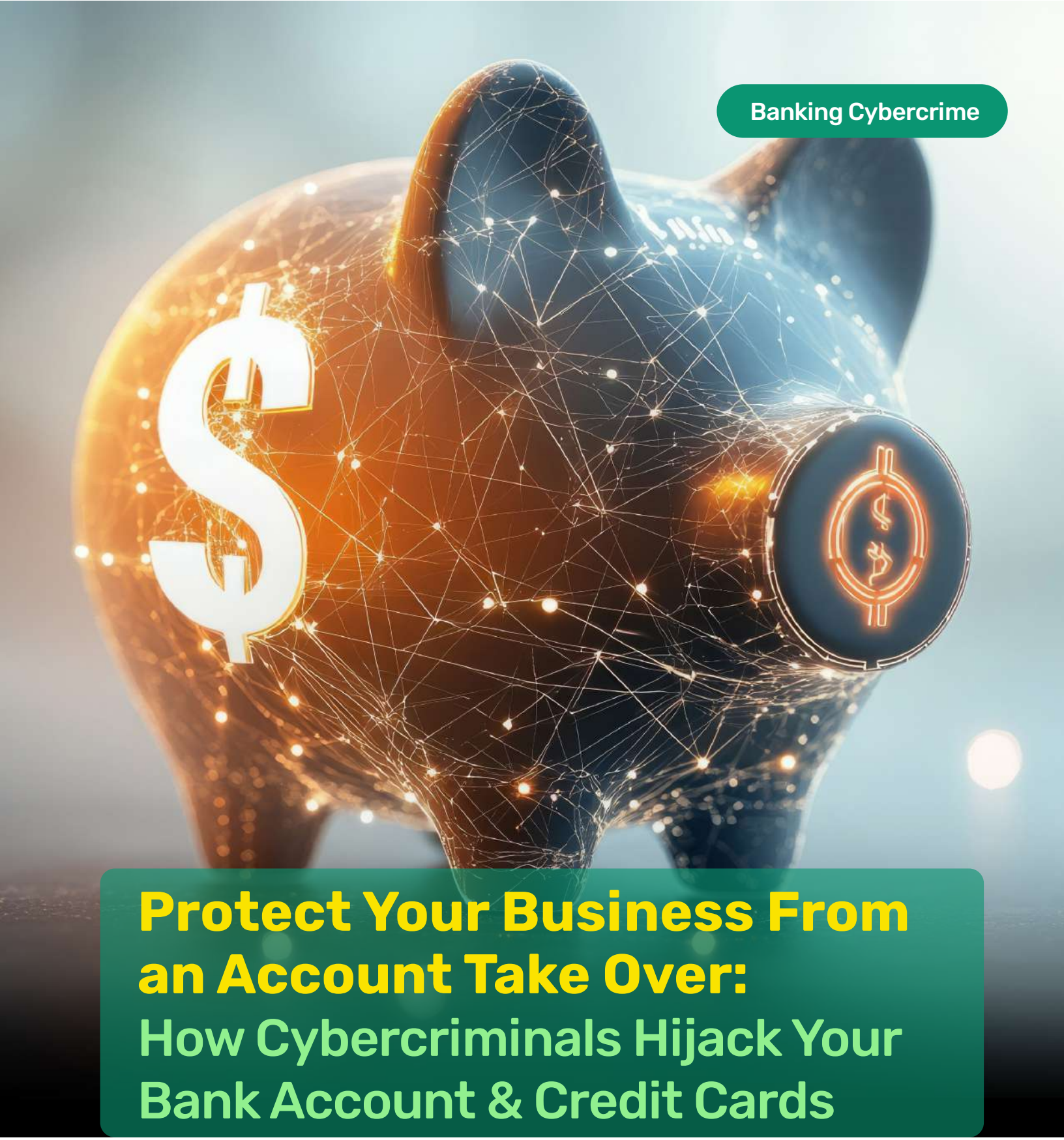


Banking Cybercrime

Protect Your Business From an Account Take Over:

How Cybercriminals Hijack Your Bank Account & Credit Cards

Reliable Resistant Secure

BULLET PROOF TECH GUIDES

Insider Tips To Make Your Business Run Faster, Easier, and More Profitably.

You've built a solid business from the ground up. You've hired a talented team and your products or services are in demand. Business is great!

And then comes a problem: Your bank accounts and credit cards have been hijacked.

Don't think it can happen to you?

According to the 2024 J.P. Morgan fraud report, **80% of organizations* experienced bank and payment fraud in 2023**, the highest rate since 2018. *Businesses of all sizes

Corporate account takeover is a type of fraud where cybercriminals gain access to a business's finances to make unauthorized transactions, including transferring funds from the company, creating and adding new fake employees to payroll, using company credit cards, and stealing sensitive customer information that may not be recoverable.

Once the hackers have access to your bank account, they quickly funnel the funds through "money mules" – sometimes unwitting and innocent accomplices who facilitate the quick redirect of the monies overseas into the hackers' accounts.

Business Bank Accounts Aren't Protected or Covered by the FDIC

Yes, you read that right. Banks have no legal obligation to reimburse businesses for attacks - federal regulations do not cover commercial accounts.

The FDIC protects account holders should there be a bank failure or a "run on the banks" during which customers rush to withdraw their funds, causing banks to collapse. The FDIC doesn't protect businesses from the repercussions of someone hacking their account and stealing their money.

Individual consumers are protected from fraudulent transfers under Regulation E of the Electronic Fund Transfer Act. This regulation puts the burden on banks to bear the financial losses of a fraudulent event. However, this regulation doesn't cover businesses, not even those owned by a single individual.

A cyber liability policy can provide some business protection in case of a bank account attack.

How Do Cybercriminals Get Access to My Accounts?

The most common techniques hackers use is "phishing" and "pharming." While some criminals still employ the "old school" methods, like stolen checks, check cards, and credit cards, most bank and credit card theft are now committed online via emails and websites.

Here are the three most common attacks/attempts to take over your business account:

1 Phishing (pronounced "fishing")

Where a cybercriminal sends an email purporting to be from a financial institution or other organization.

The email typically includes a specific call to action to get you to click on an embedded link. Common phishing phrases used are "security concerns," "too many attempted logins," and an urgent need to "authorize attempted transactions."

The entire goal of the email is to get you to confirm your personal and account information immediately to avoid some negative consequences – such as immediate account closure. The emails look official and often contain graphics stolen from the legitimate company from which the message claims to originate. With the increased use of AI, these emails have become difficult to spot.

When you click on the phishing email links, you will be taken to a spoofed website containing stolen graphics, logos, and information from the legitimate company's website.

If you attempt to log in, you have just provided the criminals your login credentials to the real website.

The website addresses used in these scams are very close to the real organization's website address. However, they often contain additional words or a series of letters and numbers not in the legitimate address.

Example: www.bankofammerica.com or www.safe.bankofamerica.com.

***Both of these examples have been used (successfully) in phishing emails.**

2 Business Email Compromise (BEC)

While considered a form of phishing, this is a highly targeted specialized attack.

A BEC attack relies on social engineering and spear phishing techniques developed by online reconnaissance (watching corporate and personal social media accounts for company team members).

Typically, cybercriminals impersonate or compromise an email account belonging to the business owner, CEO, or other individuals authorized to conduct purchasing, handle sensitive company information, or have other fiduciary responsibilities. They aim to manipulate their target into wiring funds or revealing sensitive information.

Here are a few common elements found in a BEC email:

Time sensitivity. The objective is to get the target to act quickly before they realize they are being scammed. The cybercriminals use words like 'quick,' 'urgent,' 'important,' and 'reminder.' These words appear in the subject line but can also occur inside the email.

Thorough impersonation. Emails can impersonate legitimate senders using various tactics, such as imitating the person's writing style or spoofing their email address.

Justifying the request. An unusual request can seem legitimate by providing some reason for making the request. (the person is out to lunch, at a conference, or on vacation) This tactic can convince the target to act quickly before realizing it's a scam.

Specific instructions. There are usually very clear instructions. For example, they might specify the amount of money to send and the location to make the request seem more legitimate. This information might be included in the initial or follow-up emails after the target replies.

71% of businesses experienced a BEC attack in 2024. **(Trend Micro Report)**

CEO impersonation is used in 39% of BEC attacks. Fraudsters pose as executives to authorize fraudulent transactions. **(Proofpoint Report)**

Fake invoice schemes account for 30% of BEC scams. Criminals request payments for fake services or goods. **(Trend Micro Report)**

Compromised vendor accounts are used in 29% of BEC scams. Fraudsters infiltrate trusted supplier accounts to target businesses. **(Forbes Report)**

3 Pharming

Also known as Domain Spoofing and DNS Poisoning

Is a cyberattack that tricks a user into giving away personal information by redirecting them to fake websites. It's an online fraud similar to phishing but uses malicious code instead of email.

Cybercriminals use two main types of pharming attacks:

Malware-based pharming

In malware-based pharming, internet users often unwittingly pick up malware, such as a Trojan horse or virus, through malicious email or software downloads. The downloaded malware will covertly reroute the user to a fake or spoofed website created and managed by the attacker.

When people access the site, the attacker sees all the personal data or login credentials they enter.

DNS server poisoning

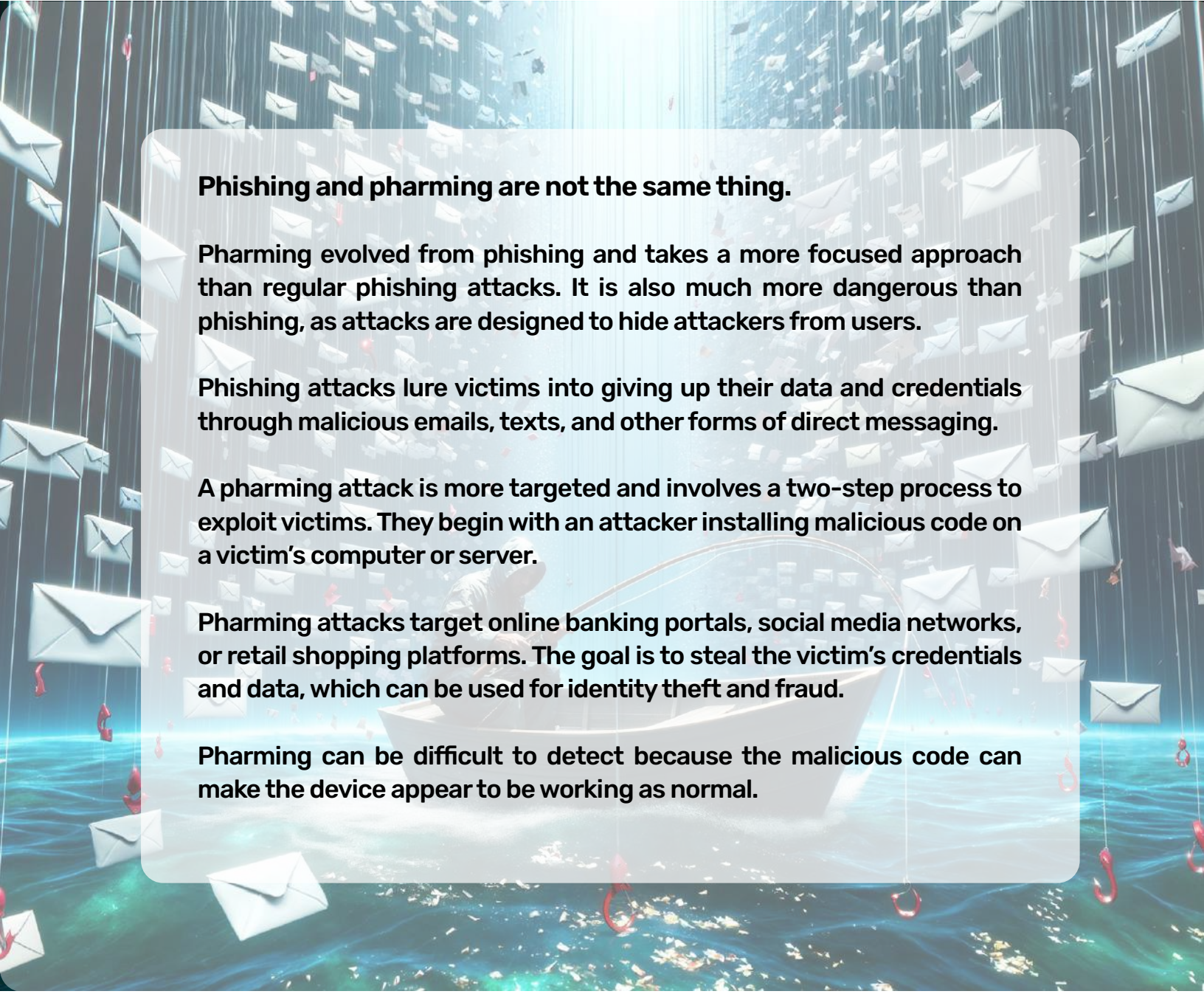
The DNS directs users' website requests to the correct IP address. However, when a DNS server is corrupted, it will direct website requests to alternate or fake IP addresses.

Cybercriminals can achieve this through DNS hijacking, which enables them to target multiple users on DNS servers and unprotected routers, especially free or public Wi-Fi networks.

***Note:** This is why you should not do banking or online shopping on free or public Wi-Fi networks.*

The No-Geek Speak of How It Works

- An attacker installs malicious code on a victim's computer or server.
- The code redirects the victim to a fake website that looks legitimate.
- The victim is tricked into giving away personal information like passwords, usernames, or credit card details.



Phishing and pharming are not the same thing.

Pharming evolved from phishing and takes a more focused approach than regular phishing attacks. It is also much more dangerous than phishing, as attacks are designed to hide attackers from users.

Phishing attacks lure victims into giving up their data and credentials through malicious emails, texts, and other forms of direct messaging.

A pharming attack is more targeted and involves a two-step process to exploit victims. They begin with an attacker installing malicious code on a victim's computer or server.

Pharming attacks target online banking portals, social media networks, or retail shopping platforms. The goal is to steal the victim's credentials and data, which can be used for identity theft and fraud.

Pharming can be difficult to detect because the malicious code can make the device appear to be working as normal.

Cybercriminals target every business, no matter the size, with these attacks.

The best defense against these attacks is your cyber security offense – using technology to protect your business proactively.

Take Advantage of Protections Offered by Your Bank

In today's digital world, most banks offer some additional protections that you can implement to help keep cybercriminals at bay.

Check with your bank - you may have to opt in or pay an extra monthly fee for some of these services.

- Use advanced monitoring. These alerts will notify you if there are signs of unusual account activity.
- Request limits on transaction sizes. Examples: cap the amount accessed in an automated clearinghouse transaction, cash advances, and ATM withdrawals. Most credit card companies also offer this option.
- Use multi-factor authentication. Require users with access to your business bank accounts to confirm their identity through a username and password and a phone call, text, or email.

A Few Best Practices in Managing Your Business' Financial Transactions

- Mandate two-employee-approval to initiate fund transfers
- Monitor your accounts regularly to catch any suspicious activity
- Don't use a check card at gas stations, fast food, or restaurants
- Limit access to business bank accounts to only essential employees
- Consider having a separate checking account or credit card that is only used for online purchases

***When possible: use a single computer for financial transactions that isn't used for internet (web) surfing.**

The Basic IT Best Practices to Keep Your Financial Data Secure

This list is the basics that every business, no matter the size should have in place.

- Use business-grade virus protection and email spam filter
- Keep computers, networks, and website browsers patched and updated
- Have a business-grade firewall that does advanced threat detection with AI
- Use mobile device management for employees with smartphones
- Leverage two-factor authentication to access vulnerable accounts
- Implement an employee cybersecurity training program
- Have an incident response and recovery plan

A Simplified Four-Step Overview of What to Do After a Bank or Credit Card Attack

While panic seems to be the most obvious reaction to your bank account or credit cards being hacked, staying calm and quickly executing an action plan will put your business on a better track.

If your business falls prey, here are the top 4 things to do:

1 **Contact your bank and credit card companies to stop further activity.**
Phone calls are better than emails at this time. Depending on the breach, using your email may not be safe. Knowing someone at your local bank is invaluable and can speed up the process.

2 **Notify your IT department and/or IT- cybersecurity provider.**
Passwords must be changed, and a scan should be done to quarantine any malware/spyware. Change any access permissions right away. Next, stop any additional data loss by taking all systems affected offline after your forensics team has conducted its analysis. Swap out any affected machines with unaffected ones. And update all user credentials and passwords a hacker may have accessed.

3 **Contact your insurance company if you have cyber liability insurance.**
Have all parties immediately write down what happened and how the attack was discovered. Refrain from destroying any evidence during the process – especially if you plan on contacting your insurance company for assistance or reimbursement.

4 **Determine if you need to contact any customers or vendors.**
The last thing you want is for the hackers to trick customers or vendors out of their money by impersonating your company.

****Optional:** File a report with the local authorities and the Federal Trade Commission (FTC). Depending on the severity of the crime and your industry, this step may be mandatory. However, for most small businesses, filing a report does little good except to help with fraud and cybercrime statistics.

When It's All Said and Done - Review What Went Wrong and Beef up Your Protection.

According to Crowstrike, 68% of companies that have been hacked will encounter another "sophisticated intrusion attempt" within 12 months.

This almost certainly won't be the last time your small business gets targeted by hackers. Once the dust has settled, review your response plan, assess what could have been done differently, and strengthen your cyber security to prevent future attacks.

Now would be a great time to perform a risk assessment on your business.

A Real Story About Business Bank Fraud

Here is a local Nashville business's real-life business banking fraud experience. I've changed the names of the individuals to protect their privacy. They were not our clients when this took place in 2024.

I am sharing their story as a sobering reality check. Your business bank account is not safe from scams and bank fraud.

John Davis owns a local roofing company with a little over twenty employees. Kimberly handles all of the company's books, including payroll, and has been with the company for over 10 years.

Last January, Kim got an email from Regions Bank stating that there had been "unusual activity" on the company bank account and requesting that she log in and review the charges before the account was put on "hold."

Kim says, "I didn't think anything of it. I was busy working on closing out last year's expenses, and I clicked the link to log in. I entered my login details and clicked the "Continue" button, and it gave me this error... it said something about an application error and to try again later."

Kim says that she returned to working in QuickBooks, and after lunch, she went to check on the bank website. This time, she did her usual thing: she typed in the bank's website address in the Google bar.

When she entered her login details, she got the "wrong user name or password" error. She tried several more times until she got the message "locked out for security reasons" from Regions.

"That's when I knew something was wrong," explained Kim.

"I got in the car and drove to our branch. That's when I learned that we had been hacked. $272,000 gone!

It was transferred to an account in Florida. By the time Regions tried to track the money, it had gone from a Regions bank to a Wells Fargo, and that account was now closed. That money vanished into thin air."

John went through all the reporting hoops – including filing a report with the FBI, who to this day have not been able to track down the cybercriminals.

Luckily for John, he had cyber liability insurance, and they could get their money back through an insurance claim.

"While our bank was helpful, they could not return our money. That's when I learned that the banks do not cover hacking or stolen money for a business." John explained. "I've made some changes. As a company, anyone working on a computer has mandatory cyber security training every couple of months."

In case you're wondering, no, John did not fire Kim. "I'm so grateful that I still have a job," Kim says. "I don't click on anything in any emails now!"

How to protect your business in today's digital world

Keeping up to date with the latest trends, threats, and best practices in online security is essential for maintaining effective defenses against cyber threats.

But it's a full-time job. Which is another reason you should consider partnering with an IT support provider (like us) to keep you secure and ahead of the curve.

We subscribe to industry publications, newsletters, and blogs to stay informed about emerging threats, new attack techniques, and security vulnerabilities. We do it so you don't have to.

And we keep our clients safe by handling the security and technology that runs their business, so they don't have to think about it.

Want an easy stress free way to protect your business? Get in touch.

CALL: 615-826-0017
EMAIL: info@gsgcomputers.com
WEBSITE: www.gsgcomputers.com

GSG Computers
Bullet Proof Your Technology