PROTECT YOUR PRACTICE FROM AN ACCOUNT TAKE OVER

HOW CYBERCRIMINALS HIJACK YOUR PRACTICE'S BANK ACCOUNT & CREDIT CARDS

A FREE REPORT

CSU COMPUTER SERVICES UNLIMITED

Imagine: You've built a solid veterinary practice from the ground up. You've hired a talented team and have many furry friends coming in for your help. Business is booming!

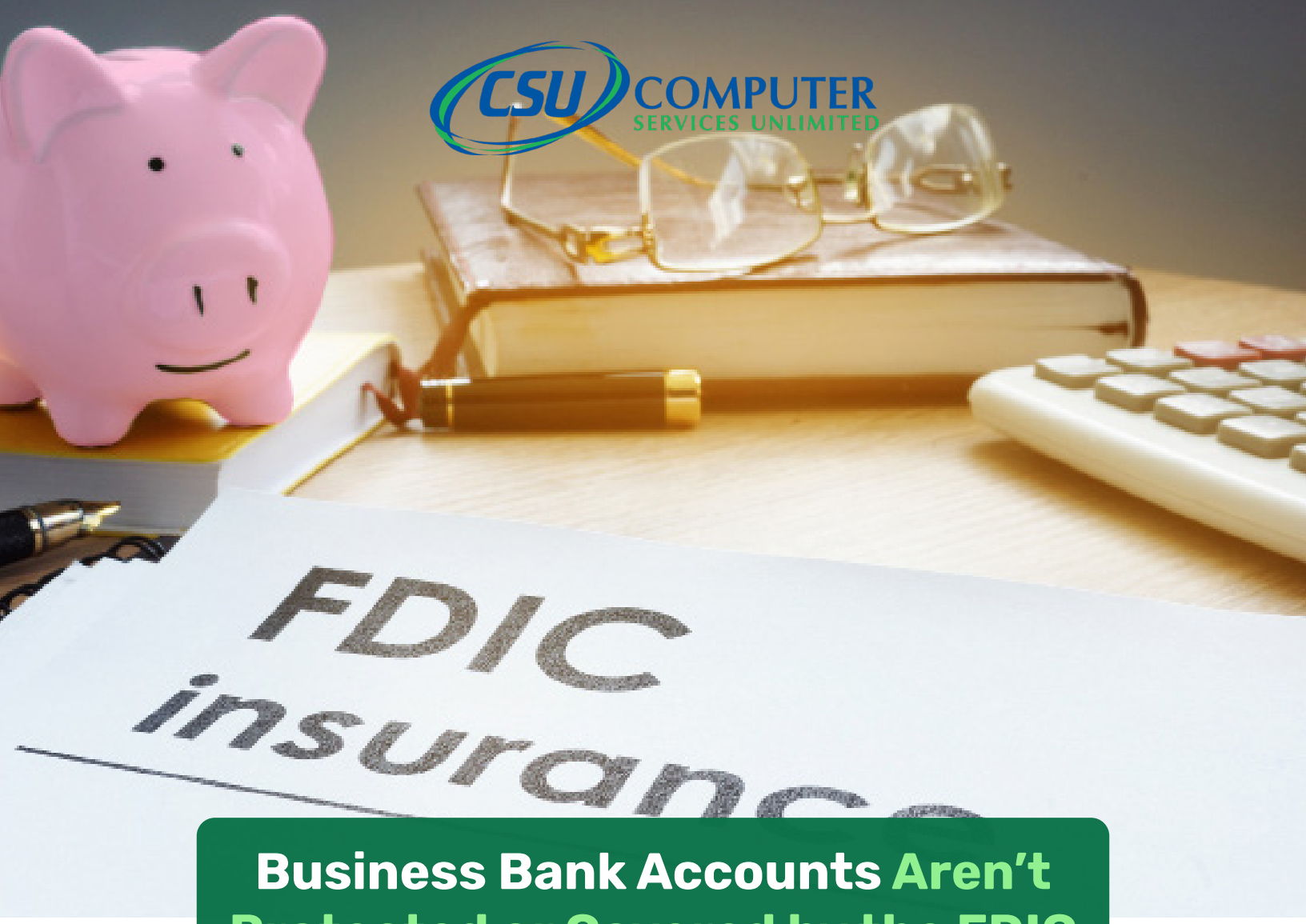
And then comes a problem: Your bank accounts and credit cards have been hijacked!

Don't think it can happen to you?

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

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 your practice 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 you from the repercussions of someone hacking your clinic's bank account and stealing that 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.

CSU COMPUTER SERVICES UNLIMITED

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 (“fishing”)

Cybercriminals send fake emails pretending to be from financial institutions or other organizations. These emails urge you to click on links to “authorize transactions” or address “security concerns” in an attempt to steal your personal and account information. They often look official, using graphics from legitimate companies, making them harder to detect, especially with AI tools.

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

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.

CSU COMPUTER SERVICES UNLIMITED

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 or industry, with these attacks.

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

3

Business Email Compromise (BEC) in Veterinarian Clinics

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

Business Email Compromise (BEC) is a targeted cyberattack, often seen as a form of phishing. It uses social engineering and spear phishing, relying on online research, such as monitoring social media profiles of veterinary staff and the practice.

Cybercriminals may impersonate or take control of the email accounts of key individuals, such as practice owners, lead veterinarians, office managers, or anyone responsible for financial transactions or handling sensitive information. The goal of these attackers is to deceive their targets into transferring funds or disclosing confidential details, putting both the practice and its clients at risk.

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

Time Sensitivity: Cybercriminals use urgent words like "quick," "important," or "reminder" to pressure targets into acting before realizing they're being scammed.

Impersonation: Emails imitate legitimate senders by copying writing styles or spoofing email addresses to appear more convincing.

Justifying the Request: Unusual requests are made to seem legitimate, often by claiming the person is unavailable (e.g., on vacation or at a conference), pushing targets to act quickly.

Specific Instructions: Clear instructions, such as specifying money amounts or locations, make the scam appear more credible.

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)**

CSU COMPUTER SERVICES UNLIMITED

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 Practice's 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 practice on a better track.

If your practice 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 practice.

****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 practices, 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 Crowdstrike, 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 practice 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 practice.

True Story...

Here is a local business's real-life experience with business bank fraud. The names have been changed for privacy. Note: this wasn't our client when this incident occurred in 2024.

This story serves as a sobering reality check that your business bank account isn't safe from scams and fraud.

John owns a local roofing company with a little over 20 employees. Kim, who's worked there for over 10 years, handles all of the company's books, including payroll.

Last January, Kim received an email from Regions Bank stating there had been "unusual activity" on the company's bank account and requested 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 closing 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 an error… 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 the bank website. This time, she did her usual thing: typed the bank's website address in the Google search bar.

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

"That's when I knew something was wrong," she explained. "I got in the car and drove to our branch. That's when I learned we had been hacked. $272,000 was gone! It was transferred to an account in Florida. By the time Regions tried to track the money, it had been transferred from a Regions bank to a Wells Fargo account, which was now closed. The money vanished into thin air."

John went through all the necessary reporting steps, 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 were able to recover the money through an insurance claim.

"While our bank was helpful, they could not return our money. That's when I learned that 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 now has mandatory cybersecurity training."

In case you were wondering, Kim was not fired. "I'm so grateful I still have a job. I don't click on anything in emails now!" Kim said.

Partnering with us, Computer Services Unlimited, means you'll receive cybersecurity training for you and your team, along with email filtering safeguards to protect against situations like this!

HOW TO STAY AHEAD OF THE CURVE

Keeping up to date with the latest trends, threats, and best practices in email 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 all the security aspects of their email, so they don't have to think about it!

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

CSU COMPUTER SERVICES UNLIMITED

14240-G Sullyfield Circle
Chantilly, VA 20151

Phone: 703-968-2600

Websites: csuinc.com, vetitservices.com, csugov.com