DollarBank

Business INSIGHTS BRIEF



INSIDE

Protecting Yourself and Your Business Against the Latest Cybersecurity Scams

Dollar Bank

Business INSIGHTS BRIEF

Every day, you are faced with decisions to help keep your business on track. Business Insights Brief provides quick hitting resources and knowledge from our banking team to help you achieve your goals.

Overview

Protecting Yourself and Your Business Against the Latest Cybersecurity Scams



Deepfakes and AI Impersonation

Compromised Passwords

Phishing, Smishing, Quishing and Vishing

Email Takeover

Ransomware

Stay informed and never let your guard down.

Protecting yourself and your business from cybercrime comes down to building your awareness of today's most common ploys and putting practical protections into place to thwart them. The Dollar Bank team is always here for you with support and solutions.

Let's talk @ 1-855-282-3888.

DollarBank®

Equal Housing Lender. Member FDIC. Copyright © 2026, Dollar Bank, Federal Savings Bank.

This article is for general information purposes only and is not intended to provide legal, tax, accounting or financial advice. The information and opinions expressed herein are subject to change without notice. Any reliance upon any such information is solely and exclusively at your own risk. Please consult your own legal counsel, accountant or other advisor regarding your specific situation.

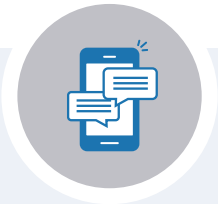
Protecting Yourself and Your Business Against the Latest Cybersecurity Scams

Keeping up with new and emerging cybersecurity scams requires constant vigilance. Scams are continually evolving, as fraudsters and criminals strive to stay a step ahead of their potential victims. They know the ins and outs of technology, and once they spot a vulnerability, they pounce on the opportunity to steal credentials, money, identities, intellectual property — anything of value.



Right now, businesses of all sizes are being heavily targeted, with attackers leaning on a mix of tactics that work at scale: convincing social engineering ploys (increasingly powered by AI), account takeover attempts aimed at email and cloud tools, and ransomware that often begins with stolen credentials or the exploitation of known vulnerabilities (unpatched or misconfigured computers, routers, etc.). Newer twists, like scams that trick you into approving a sign-in or sharing a one-time code from your phone, plus AI voice and image cloning — aka deepfakes — can make even savvy teams second-guess what they're seeing and hearing.

Information is your first line of defense. Understand the risks, put protections into place and know what to do in the event a scammer tries to engage with you. Michael Rapino, Senior Vice President, Chief Information Security Officer at Dollar Bank, shares today's most common cybersecurity risks, along with tips for protecting yourself and your business.



Deepfakes and AI impersonation

Deepfakes are becoming increasingly realistic and pose a true threat to businesses.

Deepfakes, AI-generated audio or video created to convincingly imitate a real person, are becoming a mainstream business threat as AI tools have become more accessible to scammers. A scammer may use a cloned voice to pose as an owner, a CEO or a vendor and pressure an employee to urgently send a wire, buy gift cards, change payroll details or "approve" a payment. These attacks often take the form of a phone call, voicemail, video meeting or short audio clip, and they can be paired with email or text messages that look legitimate.

How to defend your business:

- Create a "no exceptions" verification process for any request involving money, credentials or account changes.
- Have a callback policy that requires the receiver to seek verification for the request by calling a known number (not the one provided in the message).
- Require two-person approval for transfers, and use a pre-established code word or verification question for high-risk requests.
- Limit the amount of executive voice/video content posted publicly if possible.
- Train staff that hearing a familiar voice is no longer proof of identity.

Compromised passwords

Each password should be unique, and MFA is a must!

It's human nature to try to make things as easy and efficient as possible, but when it comes to protecting your information and accounts, some extra effort can pay off. Once a scammer has access to your username and password, they can wreak all kinds of havoc, from draining your financial accounts to stealing your personal information.

How to defend your business (share these tips with everyone on your team to help them keep their information secure, too):

- Use multi-factor authentication (MFA) wherever possible. If a scammer gets hold of your username or password, MFA can stop them at the gate. However, criminals increasingly use clever techniques to steal one-time passcodes (OTPs) in real time or bombard users with repeated prompts leading to "MFA fatigue" (prompting you to tap YES on the phone to make the annoyance stop). Consider using an authenticator app, and beware of OTP scams: If anyone asks you to share your code, no matter who the caller or texter says they are, don't do it. Never give anyone your OTP.
- Make every password unique. It's hard to remember a lot of passwords. That's why so many people use the same password across accounts. Huge mistake. If a cybercriminal figures out one of your passwords, they will try it across multiple accounts. Use unique passwords for every site, and when a change of password is required, use one that's strong and unique; don't change just one or two characters. Once a password has been cracked, malicious actors will try many close variations to see if they can uncover the new one. Use unique passwords for every site.
- Be careful where you store passwords. Saving passwords in your web browser is convenient, but it can also create a tempting "one-stop shop" for criminals — especially if a device is lost, shared with others, or infected with information-stealing malware designed to grab saved logins. For higher-risk accounts (email, banking, payroll, etc.), think twice before clicking "Save (or Update) login for this site?" and avoid storing those credentials in the browser. There are safer ways to keep track of passwords — namely, by creating a passphrase to help you remember or using a reputable password manager to help you generate and store strong, unique passwords. If you choose the latter, be sure to keep your master password in a secure place in case you ever forget it.



Phishing, smishing, quishing and vishing

Every employee should know how to spot red flags.

Phishing isn't new to the cyberthreat scene. Scammers have long been sending emails posing as reputable companies or individuals to deceive recipients into clicking malicious links. Those links may trigger ransomware downloads or take their victims to fraudulent sites where they are asked to provide passwords, account numbers or other confidential information.

What's new is how believable and scalable these scams have become: AI can write polished messages, imitate your vendor's tone and branding, and personalize lures using publicly available information. Many attacks now arrive via text (SMS "smishing"), QR codes ("quishing"), voice calls ("vishing"), and collaboration tools — not just email.

AI also makes scraping easy. For example, LinkedIn intentionally sets a lot of information to public (depending on your/your employees' profiles). AI empowers would-be fraudsters by scraping internet sites (looking at and grabbing whatever is publicly available). There is no breach here; this is AI simply taking advantage of what is publicly available. It can then easily correlate that data and produce lists of identities and profiles to target.

How to defend your business:

Look for red flags:

- Urgency ("do this now"), secrecy ("don't tell anyone"), and unusual payment or login requests
- Subtle changes, such as a new bank account for a vendor, a different payment portal or a "security verification" step you don't normally use
- Requests for payment via gift cards

Teach employees to:

- Slow down and verify each message and its source before they respond. If it looks or feels wrong, it probably is. They should verify the sender through another channel — e.g., call a known number for the vendor or ask their boss in person — before taking any action.
- If a message turns out to be fraudulent, other employees should be made aware of the scam so they don't fall for it, and the email address/domain or phone number should be blocked.



Email takeover

The simplest action can open the door to cybercriminals.

For many small businesses, email and cloud productivity tools (like Microsoft 365) are mission-critical, which makes them a top target. Beyond stealing passwords, criminals may try to trick someone into approving access or signing in on a page that looks legitimate. For example, you might be asked to enter a one-time code, or to click an "Approve" prompt to view a document or fix an account issue. If you do, you may accidentally give the scammer a way into your account. Once inside an email account, criminals can watch conversations, hijack invoice threads, reset other passwords and launch scams from a trusted address.

How to defend your business:

- Reduce the risk by enabling MFA for your email and any account that can move money, and never share the one-time code (or approve a sign-in) if you didn't start the login.
- Add sign-in alerts if your email provider offers them, so you know right away if someone tries to get into your account.
- Be cautious about connecting new apps to your email ("Sign in with Google/Microsoft") and a few times a year, review and remove any apps you don't recognize or no longer use.

Ransomware

Hardware and software updates are your first line of defense against malware!

Ransomware attacks continue to be a serious threat to individuals and businesses. In this type of cyberattack, criminals gain access — often through phishing, stolen credentials, exposed remote access or exploitation of known software vulnerabilities — and then deploy malware that encrypts files and disrupts operations. Many groups also steal data first and threaten to publish it if the ransom isn't paid (called "double extortion").

How to defend your business:

- Stay current with hardware and software updates, which often include security patches to address vulnerabilities. Attackers frequently exploit known flaws in VPNs, firewalls, remote access tools and other internet-facing systems because they're easy to scan for. Keep an inventory of what you expose publicly, patch those systems first, and remove or restrict remote access you don't need.
- Back up critical data and test those backups. Having a backup is vital in the event of a ransomware attack. A backup on the same computer or to an external drive that is always connected won't help; ransomware can encrypt those backups, too. Use an approach that includes at least one offline or otherwise protected copy (for example, a disconnected external drive or cloud backups with strong access controls and immutability). Just as important: Routinely test that you can restore your systems and data, so you don't discover in the throes of an emergency that backups are incomplete or unusable.

Protecting yourself and your business from cybercrime comes down to building your awareness of today's most common ploys — from AI-driven impersonation and modern phishing techniques to ransomware and cloud account takeovers — and putting practical protections into place to thwart them. Stay informed and never let your guard down.

Do what it takes to keep your assets safe.

Dollar Bank offers your business a broad range of fraud mitigation products designed to protect your accounts from unauthorized transactions, including fraudulent checks and electronic transactions. Our treasury management experts are here to help. If you'd like to discuss solutions for your business, call 1-855-282-3888, Monday - Friday 8:30 AM - 5:00 PM.

DollarBank®

Let's talk @ 1-855-282-3888.

Equal Housing Lender. Member FDIC. Copyright © 2026, Dollar Bank, Federal Savings Bank. BUS531_26