Stay Informed | Stay Secure | Stay Ahead

TECHNOLOGY TIMES

Why "Quick and Easy" Creates the Biggest Security Gaps

Passkeys Are Replacing Passwords: What to Expect Next

Passwords are finally starting to lose their grip, and that's a good thing. More platforms (especially business identity systems) are moving toward passkeys, which let you sign in using your device's built-in security, like Face ID, Touch ID, or a secure PIN. Instead of typing a password that can be stolen, passkeys use strong cryptography behind the scenes and are much harder for attackers to intercept.

Over the next several months, you'll likely see more "passkey prompts" inside Microsoft sign-ins and other major platforms. Some organizations may notice new passkey settings being introduced automatically or re-organized in their admin portals as vendors standardize how passkeys are managed.

For end users, the experience is usually simpler: you're prompted to approve sign-in on your device rather than remember another password. If your company has been dealing with login-related issues (phishing attempts, password resets, suspicious sign-in alerts) this shift is a major step forward. But like any change, it works best when it's intentional. The best implementations roll out passkeys in a controlled way, starting with a pilot group, then expanding based on real user feedback.

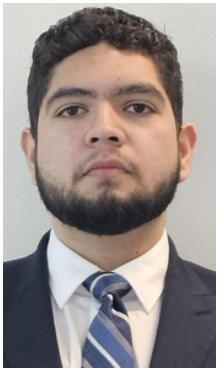
If you need help with passkeys or have any cybersecurity questions, reach out to us! We can help you stay secure and protected.

EMPLOYEE SPOTLIGHT

Employee of the Month: Caroline England

Caroline, one of our account managers, continues to raise the bar with consistent follow-through and a strong commitment to client relationships. Her drive, reliability, and results-focused mindset make a real impact for both our clients and our team. Congrats, Caroline — and thank you for bringing that momentum every day!

Tech Genius of the Month: Gerardo Lopez



Gerardo has been delivering the best standard of support, stepping up and showing up wherever he's needed. He is always known for thoughtful problem-solving, excellent client communication, and taking ownership to make sure work gets done the right way. Congratulations, Gerardo, and thank you for your dedication and initiative!

Upcoming at Vector Choice

Coming Soon: Webinar on EOS® Execution with Strety

If your EOS® tools are scattered across notes, spreadsheets, and multiple apps, keeping traction gets harder than it should be.
In just a few weeks, we're hosting a webinar on Strety, an EOS® execution platform that brings L10s, scorecards, Rocks, Issues, and projects into one connected system (with deep Microsoft Teams integration). We'll share how it helps leadership teams stay aligned, accountable, and focused, without adding more tool sprawl.

Thursday April 2nd, 2026
1:00 PM EST

QR Codes Can Be a Scam, Too

QR codes feel safe because they don't look like a sketchy link, but they can lead to the exact same danger. Scammers are increasingly using QR codes to send people to fake login pages, fake payment screens, or "download" prompts that aren't what they seem. This tactic is often called QR phishing, and it works because it feels normal: scan a code, get a result.

These scams show up in places that don't feel "cyber," like a label on a package, a flyer in an office lobby, a sign at a venue, a fake parking payment notice, or even a QR code slipped onto a legitimate poster. The goal is simple: get someone to scan, then capture credentials or payment details before the person has time to think twice.

A good rule of thumb is to treat every QR code like a link you didn't ask for. If it's pushing you to log in quickly, reset a password, confirm a payment, or "verify your account," slow down. If possible, navigate to the website directly through a trusted bookmark or by typing the address yourself instead of letting a QR code choose the destination for you.

Business Banking Fraud: Why "We'll Get It Back" Isn't a Strategy

A hard truth: when money leaves a business account due to fraud, recovery is not guaranteed. Business accounts don't always have the same protections people assume exist from personal banking experiences. That's why preventing fraud matters more than reacting to it.

Most business payment fraud isn't caused by a "hacker in a hoodie." It's caused by process breakdowns; someone receives a convincing message, a login gets captured, a vendor's email gets impersonated, or a wire request slips through without verification. The attack is usually a combination of social engineering and opportunity. It can happen anywhere and at any time.

The strongest banking security comes down to layering simple protections: multi-factor authentication on every login, real-time alerts for transactions, added verification controls for checks, and requiring more than one person to approve high-risk payments like wires. Another practical step many teams overlook: keep banking activity on a dedicated business-only device that isn't used for web browsing and email.

If you haven't reviewed your banking security features recently, this is a perfect month to do it. A short call to your bank to confirm which fraud protections are enabled (and which aren't) can make a big difference.

Client Spotlight
Coming Next Month

We're saving this spot for one of our amazing clients!

If you'd like your company featured in next month's newsletter, we'd love to highlight your team, whether it's a recent win, a milestone, a project you're proud of, or a quick "how we work together" story.

Want to claim the spotlight? Reach out to our Marketing team this week to reserve next month's feature.

Contact:
Chloe Vainrib
at cvainrib@vectorchoice.com

Tech Tips You Can Use Right Now: February Recap

1. **Phishing Shows Up Everywhere, Not Just Email**
   Modern phishing can hit through texts, social DMs, collaboration tools, QR codes, and even phone calls. When something feels urgent or unusual, slow down and verify through a separate channel (call a known number, start a new message thread, etc.). If you're unsure, forward it to us — we'll help you confirm what's real.

2. **Don't Store Passwords (Or Cards) In Your Browser**
   Browser-stored passwords can be easier to expose than most people realize. A professional password manager helps you use strong, unique passwords without the headache — and reduces the fallout if one account gets compromised.

3. **Antivirus Isn't Enough Anymore. You Need Behavior-Based Protection**
   Browser-stored passwords can be easier to expose than most people realize. A professional password manager helps you use strong, unique passwords without the headache — and reduces the fallout if one account gets compromised.

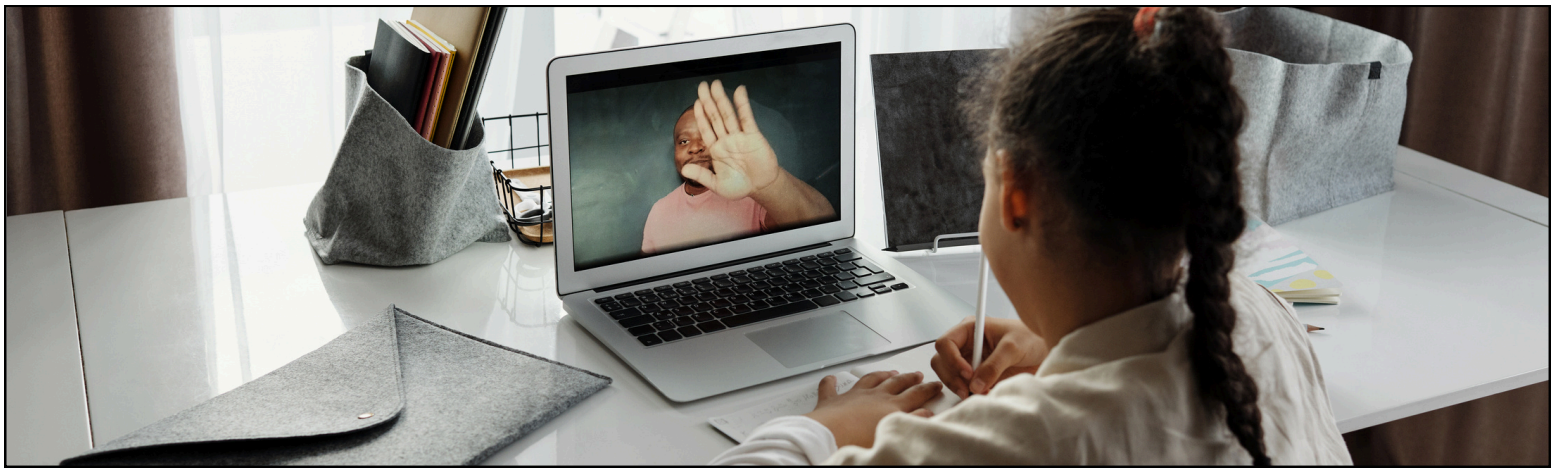
4. **Business Banking Fraud is a Different Game**
   Business accounts often don't have the same protections as personal accounts. Key steps include MFA for every login, real-time alerts, positive pay, and dual approval for wires. Also: keep banking to a dedicated, business-only device and ask your insurance broker about cyber fraud coverage.

Want the March tech tips before next month's recap?

Sign up for our weekly tech tip emails now by scanning the QR code below:

(Don't worry, this one is safe)

Online Safety for Kids: The Simple Habits That Make the Biggest Difference



Online safety can feel overwhelming because it's not one app, one setting, or one conversation. It's a series of small choices that add up, especially as kids get older and technology becomes more social, more mobile, and more private.

The most effective approach is to combine a few practical layers:

- Clear expectations about what's okay to download, click, and share
- Age-appropriate apps and messaging platforms
- Basic device restrictions that reduce explicit content and unwanted contact
- Regular check-ins that don't feel like interrogations

Kids are smart, and the internet is persuasive. The goal isn't to "lock everything down" forever, it's to make risky situations less likely and to build a habit of speaking up when something feels off. Even one family rule like "If it makes you feel weird, show me" can prevent a lot of damage.

If you missed it, last month we hosted a live webinar on the topic: Keeping Your Kids Safe Online. In this live session, we covered practical ways to protect your kids online, plus how self-esteem, open communication, and the right resources play a huge role in online safety.

The webinar included:

- The most common online risks for kids today (and what to watch for)
- Simple settings and habits that reduce risk without constant monitoring
- How to start conversations that keep kids honest and engaged
- Where to find trustworthy resources when something feels "off"

If you missed the webinar, no worries! Watch the full recording now by visiting our website: **https://vectorchoice.com/webinars**

About the Host

Mike Bazar, President

As a business leader and dad, Mike is focused on helping children, families, and organizations stay safer in today's digital world. Mike shares practical guidance and points to trusted resources you can rely on.