A new favorite tool for scammers

QR codes have become part of everyday life. You see them on menus, posters, ads, even parking lots. They're quick, convenient, and we've all got used to scanning them without much thought.

But that's exactly why criminals have started hijacking them.

This type of scam is called quishing. It's short **for "QR code phishing".**

Instead of clicking a suspicious link in an email or text, you scan a code that takes you somewhere you shouldn't be. It might send you to a fake payment page, trick you into handing over login details, or even try to install malicious software on your phone.

The tricky thing about QR codes is that you can't see what's behind them until you scan.

And it doesn't take much for scammers to cause damage. Some simply stick their own QR label on top of a genuine one, often in places like parking lots, bus stops, or shop windows.

Others send scam emails that look official but hide a dangerous code inside.
These scams usually rely on creating urgency. Telling you that your account is at risk, a payment is due, or an offer is about to expire. In the rush, many people don't stop to check before scanning.

And that's exactly what the scammers want.

The best protection is vigilance. Be cautious of QR codes in unexpected emails or messages. And if you're asked to log in or make a payment, go to the website directly instead of scanning.

In public spaces, look carefully at physical codes before scanning them. If a sticker looks tampered with, don't scan it.

And if you do scan, always double-check the website address before entering any personal information.

QR codes are here to stay, and most are safe. But now that criminals are exploiting them, it pays to pause and think before you scan. That goes for your teams too. A little bit of caution could stop your data - or your money - from ending up in the wrong hands.

If you'd like to keep your team up to date with the latest cybersecurity risks to watch out for, we can help.
Get in touch.

?A

Q: Do we need to back up data stored in Microsoft 365 or Google Workspace?

A: Yes. These services keep things running, but you're still responsible for your data. Backups protect against accidental deletion or ransomware.

Q: Our passwords are strong. Do we still need multi-factor authentication (MFA)?

A: Absolutely. Even strong passwords can be stolen. MFA adds an extra layer of protection that makes accounts much harder to break into.

Q: Should we worry about old staff accounts once someone leaves?

A: Yes. If ex-staff logins aren't closed, they're open doors for attackers. Always remove access right away.

Business gadget of the month

KeySmart TaskPad

You know what a distraction it can be when your devices all need charging at your desk. Cables everywhere.

But it doesn't have to be that way. The KeySmart TaskPad charges your phone, laptop and tablet when they're placed on it. No cables. And not only that, it makes using a mouse smoother, and it's even water-resistant, anti-scratch, and stain-proof.

Hello clean and tidy desk.

$49.99 from Amazon.

This is how you can get in touch with us:
CALL: (661)-750-8402 | EMAIL daniel@goldenhillsit.com
WEBSITE: www.goldenhillsit.com

Golden Hills IT

NOVEMBER 2025

Your monthly newsletter, written for humans not geeks

TECHNOLOGY INSIDER

Your **best defense** against a cyberattack

Cyberattacks rarely make headlines when they hit SMBs. But behind the scenes, they're happening every day.

In fact, while you're reading this, somewhere a company is quietly dealing with the fallout of being locked out of its own systems.

What separates the businesses that recover quickly from those that don't isn't luck. It's preparation.

Hackers have become very good at sneaking in, stealing data, and causing disruption. Even strong security can't block every attempt. That's why having a recovery plan matters so much.

A disaster recovery plan is simply a playbook for your business. It sets out what happens if the worst occurs:

- **Who takes charge**
- **How you communicate with staff and customers**
- **The steps to bring systems back online**

When people know what to do, they can act fast and confidently rather than wasting precious hours figuring it out on the spot.

Security experts (like us) often run practice scenarios, pitting "attackers" against "defenders". What becomes obvious in these exercises is that the technical side of an attack is only half the battle.

Clear communication, calm decision making, and having tested plans ready to go make the biggest difference in whether a business survives intact.

Preparation also means knowing where your vital data is stored, making sure backups are reliable, and checking that everyone understands their role if trouble strikes. And sorry to be the bearer of bad news, but these aren't one-time jobs. You need to revisit and test them regularly.

The reality is that cybercriminals aren't going away. But you can take the fear out of the unknown by being ready.

Preparation turns a crisis into something manageable, helping you protect your data, your reputation, and your customers' trust.

If you need expert help creating a plan for if things go wrong, my team and I are on hand. Get in touch.

DID YOU KNOW...

you can download to a bird?

A musician and science enthusiast recently tried storing data in a starling. Yes, a bird.

He encoded an image into sound and played it repeatedly to the starling. Later, it appeared to reproduce a similar waveform on its own, equivalent to "176 kilobytes of uncompressed data".

While it's more curiosity than breakthrough (after all, your files could literally fly away), the experiment shows just how strange the intersection of biology and technology can get.

TechFacts

1 Researchers found flaws in McDonald's McHire job chatbot that could have exposed data from 64 million applicants. One issue? An admin password set to "123456"🙄Combined with a coding bug, it left names, addresses, and even chat messages at risk. The problem was fixed quickly, but it's a clear reminder of why strong passwords and good security practices matter.

2 AI takes a lot of power. So much that US data centers looks to become the world's fifth-largest electricity users by 2026. Microsoft, racing to fuel its AI growth, is spending $80 billion on energy infrastructure while also pledging to be carbon-negative by 2030. To offset emissions, it's buying carbon removal credits, including burying millions of tons of waste deep underground.

3 In August 1991, astronauts aboard Space Shuttle Atlantis sent the very first email from space, using an Apple Macintosh Portable. With some tweaks to NASA's comms system, the bulky Mac connected to Apple's online network, AppleLink. Astronauts Shannon Lucid and James C. Adamson's message? A cheerful "Hello Earth!" complete with a Terminator 2 reference: "Hasta la vista, baby… we'll be back!"

INSPIRATIONAL QUOTE OF THE MONTH

"Courage doesn't always roar. Sometimes courage is the little voice at the end of the day that says, 'I'll try again tomorrow'."

Mary Anne Radmacher, writer and artist.

Technology update

We could soon see an AI-centric Edge

Microsoft has been experimenting with a new look for its Edge browser, known as Olympia. The prototype design puts Copilot, the built-in AI, right in the middle of the address bar and adds features like voice search and vertical tabs.

Although Microsoft seems to have moved away from this design, parts of it can still be found in test versions of Edge, showing how the company may reshape the browser around AI in the future.

November is here – time for another fun tech quiz

1. Bing is a search engine developed by what company?
2. What is another name for a URL saved in a web browser?
3. A "Page Not Found" error on a website is also known by what error code?
4. Microsoft Word's native file format uses what file extension?
5. What is the standard Windows keyboard shortcut for the Cut command?

The answers are below.

1.Microsoft
2.A bookmark
3.404
4.docx
5.Control + x

NEW TO

MICROSOFT

Excel can read pictures

Excel has a new trick: It can now analyze pictures as well as numbers.

You can drop an image into a cell, and Excel will help check things like whether it's clear or blurry. This could be useful if you work with lots of photos or scanned documents and need a quick way to spot problems before sharing them.

Behind the scenes it uses Python (a popular programming language), but you don't need to be a coder to benefit. The update is starting to roll out for Microsoft 365 users on web, Windows, and Mac.