ANYWAY TECHNOLOGIES

205 E. MERRIMAN AVE.
WYNNE, AR 72396

## Top News Inside



## How Phishers are Weaponizing QR Codes

Quishing: It may sound like a funny word, but the danger posed is anything but a joke.

QR Code phishing, also known as ***quishing***, has impacted victims around the wolrd. QR codes have been around, but the 2020 pandemic really launched a global shift toward codes instead of physical copies.

In many ways, the practice makes sense. In the years since COVID-19 struck, we've continued to embrace QR everywhere from restaurants to fliers posted around town. They make it easy to track visitors and interested parties, they're automatically updated whenever you change the website, and they significantly reduce printing costs and the time taken to distribute whatever information the QR code contains. It's no surprise that QR has flourished.

Unfortunately, that gives cyber-attackers the perfect opportunity to sneak malicious links and content. You don't know what's behind the QR until you scan it, and by then you may have already been redirected to a dangerous website or infected with malware or ransomware.

NEVER scan QR codes unless you know where it came from and where it goes! Check the URL that pops up when you scan, before using a QR code that could be out to get your data and devices.



Monthly
# Newsletter

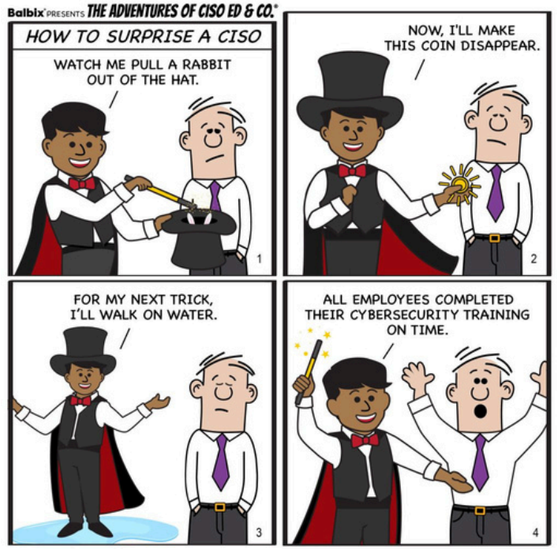
August 2024 Issue #8

*What should you do when you find corrupted backup files? Discover a virus? Get hit with ransomware? We have answers to ALL your tech questions!*

## CAUGHT IN A CYBERCRIMINAL'S WEB OF LIES?

Bringing you the monthly scoop on information security.

From the tricks hackers are using against you right now, to the best digital defenses available, to small ways you can protect your accounts every day, we're here to bring you up-to-date news on cyber-safety!




*"I'll have to see it to believe it."*

## THE MORE YOU KNOW

### Did You Know?

**Breaches involving healthcare data are the costliest, averaging nearly $11M per attack.**

Your private health information, often known as *PHI*, make up some of the most lucrative personal records for sale on the Dark Web.

Healthcare breaches are no joke! Do you know how well your health providers are protecting your important personal data?

## Why Does Cyber-Compliance Matter?

Cyber-compliance might sound like a big business issue, but it's really anything but!

How much have you heard about cyber-compliance? How well do you know the status of your own personal cyber-compliance...and do you even know why it matters so much?

It's not just about *what* regulations protect your private data, but also how much is secured under the law, and what will happen if that confidential information is ever exposed unlawfully.

Consider it: Most businesses store your data, like email addresses, full names, shopping habits and even financial information. Compliance ensures that all of these companies protect your private data with physical and digital safeguards.

Data breaches aren't just scary or frustrating, because of possible identity or financial theft.

Cyber incidents also take up a lot of time and energy. They often lead to fines and lawsuits, ensuing legal fees and plenty of your time. If you could guarantee that you only do business with reputable companies that take your data's privacy very seriously, then you can be much more comfortable entrusting your personal and financial information with them.

In other words? ***Their compliance is critical to your internet protection.***

So, maybe you aren't the CEO or owner...but you still affect its overall cyber-compliance! YOU could be held liable for intentional negligence and failure to abide by compliance regulations. Abiding regulations will help you avoid legal, reputational and financial headaches.

Data management requires transparent, trustworthy and strategic solutions.

Cyber-compliance isn't just about following rules – it's about protecting you and your data in the digital world!


### Outsmart Financial Scammers

The more easily accessible our banks and finances become, the more chances that cybercriminals have to lure us into complex and devastating financial scams.

What are some of the most common financial scams and how you can protect yourself?

**Phishing** is a classic scam involving emails or texts that appear to be from legitimate sources like banks, credit card companies, or even government agencies. They often create a sense of urgency, making you panic thinking that you're being hunted by law enforcement or deeply in debt.

Then there's **vishing**, or voice phishing, which occurs over the phone. You might be familiar with the nonstop robocalls that you get near election season and tax day; a lot of those are scammers trying to get your personal information.

**Fake checks** are also a problem. Scammers might send you a check for more than the agreed amount, asking you to return the difference. Then the initial check bounces, leaving you out the money you "returned."

The same scam has moved to Venmo, when someone links a stolen credit card and sends you money, then reaches out claiming it was a mistake. They ask you to send the money back to their Venmo. Once the credit card owner disputes the stolen charge, Venmo takes that amount out of your account....but the thief has already run off with the money you sent them.

Remember to remain skeptical! If an offer seems too good to be true, it probably is. Avoid suspicious links from unknown senders, and keep your software updated to protect yourself against zero-day attacks. Finally, use complex, unique passwords for all your accounts and enable two-factor authentication when available! Staying cybersecure is a daily effort that keeps all of us protected.



### PHI Compliance Explained

Do you work for or with a healthcare organization?

When is the last time you visited a doctor or asked for more information about your insurance plan?

This kind of data is called *protected health information* (PHI), and no matter where you live, it's protected by complex law. The exact regulations will vary by locale, but the basic rights afforded patients don't vary.

As a typical patient, you can expect the right to...

- approve when, how much of, and to whom your data is shared
- decide how your PHI is managed
- request changes to your data
- the reasonable expectation of privacy

In other words, your healthcare provider can't disclose, edit or otherwise use your personal healthcare data without your express, written permission.

The U.S. government identifies 18 categories of PHI, but the specifics therein may also vary across legislations. Nonetheless, some basic PHI identifiers include...

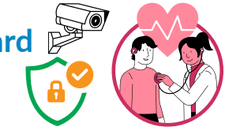
- Patient name
- Address/location
- Phone or fax info
- Dates (birthday, intake and discharge, etc.)
- Health insurance
- Account/Social Security Numbers
- Biometrics
- Vehicle info
- Medical devices

These are just a few factors of PHI, and there's even more private information protected under healthcare privacy laws.

Where do you live? When is the last time you updated your preferences regarding who can see and use your health data?

Cybercriminals consider PHI to be very valuable...so you need to know it's as safely and compliantly protected as can be!

## Are You Helping Safeguard Data Around the World?



All around the world, it can be difficult to keep your systems and devices safe from cybercriminal activity. Countries and organizations are working together more to share threat intelligence and fight cybercrime.

So how can normal people like us contribute to this global cybersecurity effort?

Start with **cyber hygiene**, the foundation of online safety. Cyber hygiene refers to the practices and steps that users of computers and other devices take to maintain system health and improve online security. It's like personal hygiene, but focused on your digital well-being.

By using strong passwords and updating them regularly, being cautious about clicking on links or opening emails from unknown senders.

Keeping software up to date with security patches also makes it harder for attackers to target you.

Remember, ***knowledge is power!*** By practicing good cyber hygiene, you can significantly reduce your risk of falling victim to cyberattacks and protect your data, privacy, and finances online.

- ✓ Use strong passwords and multi-factor a uthentication.
- ✓ Beware of phishing and social engineering s cams.
- ✓ Use secure browsing habits and browsers.
- ✓ Regularly back up your data and check that storage systems are working correctly.
- ✓ Keep your systems and software up to date.

When we make a concerted effort toward cyber hygiene, we make a more secure online environment for all!