TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's New

We want to let you know that our office is still open and operational and ready to serve you. To minimize potential exposure both to our staff, our clients and their associates, we will be following the CDC guidelines to limit all onsite support travel to essential situations only.

Options to create a support ticket:

- Tray Icon (Life Preserver)
- Email: help@imsnetworking.com
- If it's an emergency, call the support line at 701-566-5555

December 2020

This monthly publication provided courtesy of Rick Johnston, President of Information Management Systems

"Transforming Business Technology Into Systems That 'Just Work'"

QR Codes: A Sneaky Security Threat

If it seems like QR codes have popped up everywhere these days, you're right. Ever since they were first used by the Japanese auto industry to streamline manufacturing processes, companies everywhere have capitalized on the benefits of QR codes. They're cheap to deploy and can be applied to almost anything — which is why every industry from retail to healthcare is now using them as a quick and easy way to link people to websites, promotional campaigns, store discounts, patient medical records, mobile payments and a whole lot more.

QR codes aren't just cost-effective and simple to use. They're also essential, especially during a pandemic where contactless transactions have become the norm. What's more, at least 81 percent of Americans now own a smartphone, and nearly all of those devices can natively read QR codes with no third-party app required. So, QR codes are clearly having their moment.

What the Numbers Say (Hint: It's Not Good)

MobileIron, wanted to better understand current QR code trends, so in September they conducted a survey of more than 2,100 consumers across the U.S. and the U.K. It confirmed that QR codes are indeed more widely used today. For instance, in the last six months, more than one-third of mobile users scanned a QR code at a restaurant, bar, retailer or on a consumer product.

The results also highlighted some alarming trends: Mobile users don't

really understand the potential risks of QR codes, and nearly three-fourths (71 percent) of respondents can't tell the difference between a legitimate and malicious QR code. At the same time, more than half (51 percent) of surveyed users don't have (or don't know if they have) mobile security on their devices.

Like so many things that feel like they've been part of our lives forever, we don't give QR codes much thought. Mobile devices have conditioned us to take quick actions — swipe, tap, click, pay — all while we're distracted by other things like working, shopping, eating (and unfortunately, yes, driving).

This is exactly the kind of implicit trust and thoughtless action hackers thrive on. And it's why, if mobile employees are using their personal devices to access business apps and scan potentially risky QR codes, enterprise IT should start taking a much closer look at their mobile security approach.

So What, Exactly, Are the Risks of QR Codes?

Hacking an actual QR code would require some serious skills to change around the pixelated dots in the code's matrix. Hackers have figured out a far easier method instead. This involves embedding malicious software in QR codes (which can be generated by free tools widely available on the internet). To an average user, these codes all look the same, but a malicious QR code can direct a user to a fake website. It can also capture personal data or install malicious software on a smartphone that initiates actions like this:

- **Add a contact listing:** Hackers can add a new contact listing on the user's phone and use it to launch a spear phishing or other personalized attack.
- **Initiate a phone call:** By triggering a call to the scammer, this type of exploit can expose the phone number to a bad actor.
- **Text someone:** In addition to sending a text message to a malicious recipient, a user's contacts could also receive a malicious text from a scammer.
- **Write an email:** Similar to a malicious text, a hacker can draft an email and populate the recipient and subject lines. Hackers could target the user's work email if the device lacks mobile threat protection.
- **Make a payment:** If the QR code is malicious, it could allow hackers to automatically send a payment and capture the user's personal financial data.
- **Reveal the user's location:** Malicious software can silently track the user's geolocation and send this data to an app or website.
- **Follow social-media accounts:** The user's social media accounts can be directed to follow a malicious account, which can then expose the user's personal information and contacts.
- **Add a preferred Wi-Fi network:** A compromised network can be added to the device's preferred network list and include a credential that automatically connects the device to that network.

Easy Things We Can All Do to Minimize the Risks
As scary as these exploits are, they aren't inevitable. Educating users about the risks of QR codes is a good first step, but companies also need to step up their mobile security game to protect against threats like spear phishing and device takeovers.

What Users Can Do

Take a good look first: If you're scanning a QR code that's supposed to take you to a legitimate website, how can you be sure that it's actually taking you to a safe place? If you're using the QR code-scanning feature built into your default camera app or many other run-of-the mill scanning apps, the unfortunate reality is that you can't be sure. Fortunately, there are free apps that will scan QR codes and tell you if the site they're sending you to is safe or not.

Only scan codes from trusted entities: Mobile users should stick to scanning codes that only come from trusted senders. Pay attention to red flags like a web address that differs from the company URL — there's a good chance it links to a malicious site.

This article was posted in ThreatPost by Brian Foster, to read more go here: https://threatpost.com/qr-codes-sneaky-security-threat/159757/

Shiny New Gadget Of The Month:

SelfieSpin360 For GoPro

A GoPro camera is great for a crystal-clear, wide-angle video of yourself or your subject, and you can attach it to the end of a selfie stick for some nice static shots, too. But if you're ready to take things up a notch and capture even more truly awesome moments, then you need the SelfieSpin360.

It's all there in the name: the SelfieSpin360 gives you a way to get incredible 360 degree footage of yourself in any setting. You attach your GoPro or smartphone to the end of a sleek and secure base, which is attached to a long cord with a handle for camera controls on the end. Hit Record, then start swinging the device up and around your head lasso-style to capture a unique version of yourself in a special moment. The SelfieSpin360 kicks boring old selfies to the curb. Visit SelfieSpin360.com to purchase yours.

New Phishing Attack Uses Unique Method To Avoid Security

Hackers are always looking for a new angle, and recently, they've found a particularly good one.

Image recognition software is becoming increasingly sophisticated. So if hackers are interested in building a fake landing and login page designed to spoof some other company, they have to get it exactly right, including the background image, or most AV software will see through the ruse.

To get around that, some clever hackers have taken to building two different landing pages; one for the AV software and one for the user.

The page designed for the software uses the proper background image, but with the colors inverted. Image recognition software looks primarily for shapes and not for colors, so this easily fools most AV software. If a site visitor were to see that page, however, they would instantly see the flaw and become suspicious, so they're directed to a different version of the page with a proper image.

Recently, a research team attached to WMC Global had this to say about the new technique:

"Our team reviewed other campaigns deployed by this threat actor, discovering that the individual was using the same inversion technique on the newer Office 365 background."

If you're an Office 365 user, it pays to play close attention to the URL of the page you're navigating to, so you can improve your odds of avoiding inadvertently giving your login credentials to a group of hackers.

Naturally, Office 365 isn't unique in this regard. You can bet that hackers around the world are employing this trick to gain login credentials all across the internet, so vigilance is absolutely called for.

Kudos to the team at WMC Global for spotting the new trend, and make sure your IT staff is aware of the possibility so they can be on high alert and work to protect your users.

Bits & Bytes

Top Business Apps To Get You Organized

If you're struggling to stay on top of your work tasks, there are some great apps available to help out.

- **Asana** helps your business improve communication and collaboration. You can view all tasks and projects and follow progress on a communal board so you can communicate without having to rely on e-mail.
- **Proven** helps organize your hiring process by posting listings to multiple job boards with one click. You can also review and sort applicants with ease.
- **Boxmeup** organizes and tracks your packages, containers and bulk storage items to make storing and shipping a breeze.
- **Evernote** keeps all your notes organized in one place and allows you to easily share notes and lists with co-workers.
- **Trello** tracks your team's workflow. Whenever you make a change to a project or task, the app notifies each team member involved so you don't have to.
- **KanbanFlow** helps managers visualize overall workflow. It gives overviews of work status, tracks progress and assigns tasks to team members. *Nerdwallet, Apr. 21, 2020*

Top 5 Ways To Overcome Setbacks and Grow

After you encounter a setback, it can be hard to start again. But simply believing in yourself is the best way to get back on track.

1. Recognize when failure is your fault and when it isn't. Some setbacks are entirely out of your control. Learn to recognize the difference in your faults and what you can't control, then move forward.

2. Learn from your mistakes and don't repeat them. Immediately letting go of the regret of making a mistake can be hard, so instead, focus on what caused the mistake, then learn from it.

3. Focus on your new goal. Failure often comes from going after something we don't truly want. Discover what you really want so you understand what you need to work on.

4. Celebrate small wins. You don't have to wait to celebrate, even if you haven't reached your end goal. Validate yourself for completing smaller tasks, and you'll empower yourself to keep going.

5. Find the right mentor. This is someone who believes in you, even when you don't believe in yourself, and who can support you in reaching your goals. Find someone with the right knowledge and experience to learn from. *Business Insider, Sept. 16, 2020*

Windows 10 Tip: Cut Down On Distractions With Focus Assist

It's frustrating to try and get work done when you keep getting interrupted with notifications. You can determine how many you get with Focus assist, a tool Windows 10 added in the April 2018 update.

Set it up by going to Settings > System > Focus assist. Choose from three options: Off (get all notifications from your apps and contacts), Priority (see only selected notifications from a priority list that you customize, and send the rest to your action center), and Alarms only (hide all notifications, except for alarms).

You can also choose to automatically turn this feature on during certain hours, or when you're playing a game.