SECURITY INSIGHTS:

Scammers are Using QR Codes to Trick You

Genady Vishnevetsky, Chief Info Security Officer, Stewart Title Guaranty Company

QR-Code-based attackers ("quishing") have been on hackers' radar since inception. Like anything else in the cyber world, attackers continuously modify their attack vectors and social engineering techniques to get to their destination - you. Let's see what has changed.

- Scammers hope you'll scan the code on your **personal phone**, which might not have the same strong security as a work computer
- They **embed QR Code inside** the PDF or Word documents to evade email security technologies
- They often use topics that make you want to act fast, like a fake **payroll update** or a document you supposedly need to sign
- Sometimes, the QR code doesn't take you straight to the fake website. Instead, it might bounce you through one or more **legitimate websites** before finally landing on the scam page
- They might even use **human verification** steps, like those "I'm not a robot" checks you sometimes see online, to fool security systems
- When you land on the fake login page, your **email address might already be filled in**. They use personalized company branding. This makes it look even more real and might trick you into just entering your password
- They might even have systems that **reject fake passwords** and show error messages, meaning they are likely targeting specific people or companies

TAKEAWAYS:

- **Be very cautious about scanning QR codes** from emails or documents you weren't expecting
- If you receive a message asking you to scan a QR code, **stop and think** if it makes sense
- Even if the email or document looks like it's from a company you trust, **be wary** if it's unusual
- If your phone shows you a website address after scanning a QR code, **take a close look** before you proceed. Does it look like the real website you expect?
- **Never enter your login information** on a website you accessed through a QR code unless you are absolutely sure it's legitimate
- If you think something is suspicious, **it's always best to go directly to the company's website** by typing their address into your browser instead of using the QR code