QR Code Phishing: The Rising Threat and How to Stay Safe

Published 11/23/2023 by Giuseppe Aloisi

Earlier this week, we conducted a simulation by sending an email that encouraged you to click on a QR code. Did you happen to engage with it? Rest assured, this was a test aimed at educating students on common phishing scams, but if you did click on the code, we recommend taking a moment to learn more about this phishing scam technique.

In our increasingly digital world, QR codes have become a part of our daily lives. From restaurant menus to event tickets, QR codes are convenient tools for accessing information quickly and easily. However, with their rising popularity, cyber criminals have found new ways to exploit this technology. QR code phishing attacks are on the rise and it's crucial for users to be aware of this threat to protect themselves from falling victim to scams.

Understanding QR Code Phishing

QR code phishing is a type of cyber attack where malicious QR codes are used to trick users into revealing sensitive information or downloading malware onto their devices. These deceptive codes can be placed on physical objects, websites, or even sent via email or messaging apps. When unsuspecting users scan the QR code, they are redirected to a fraudulent website or prompted to download a malicious app.

Why QR Code Phishing is Popular

Several factors contribute to the increasing popularity of QR code phishing attacks:

1. Widespread adoption of QR codes: The COVID-19 pandemic accelerated the adoption of QR codes for contactless interactions, making them more common in everyday life
2. Anonymity: Cybercriminals can easily create and distribute QR codes without revealing their identity, making it challenging to track down the perpetrators
3. Social engineering: QR code phishing often relies on social engineering techniques, such as using enticing offers or urgent messages to lure victims into scanning the code
4. Mobile device dependency: Most people rely heavily on their smartphones, making

them more susceptible to QR code-based attacks as they are more likely to scan codes without thinking twice

How to Protect Yourself from QR Code Phishing

Being aware of the threat is the first step toward protecting yourself from QR code phishing. Here are some tips to help you stay safe:

1. Be cautious: Treat QR codes like you would any other link or URL. Only scan codes from trusted sources and if in doubt, don't scan them
2. Check the URL: Before scanning a QR code, inspect the URL it leads to. If it looks suspicious or doesn't match the expected destination, refrain from scanning it
3. Use a QR code scanner with built-in security: Consider using a QR code scanner app that offers security features, such as URL validation and malware detection
4. Keep your device updated: Regularly update your smartphone's operating system and apps to ensure you have the latest security patches
5. Enable two-factor authentication (2FA): Enable 2FA wherever possible to add an extra layer of security to your accounts. Even if your password is compromised, 2FA can help protect your accounts from unauthorized access
6. Educate yourself: Stay informed about the latest cybersecurity threats, including QR code phishing, so you can recognize potential dangers when you encounter them
7. Report suspicious codes: If you come across a QR code that you suspect is malicious, report it to the relevant authorities or the platform where you found it. Use the report phish button

Conclusion

QR codes have simplified various aspects of our lives, but their widespread use has also made them a prime target for cybercriminals. QR code phishing is a growing threat that can have serious consequences for individuals and organizations. By staying vigilant, being cautious when scanning QR codes and following best practices for online security, you can protect yourself from falling victim to these deceptive attacks. Stay informed, stay safe and always think twice before scanning that QR code.

tags : student-news