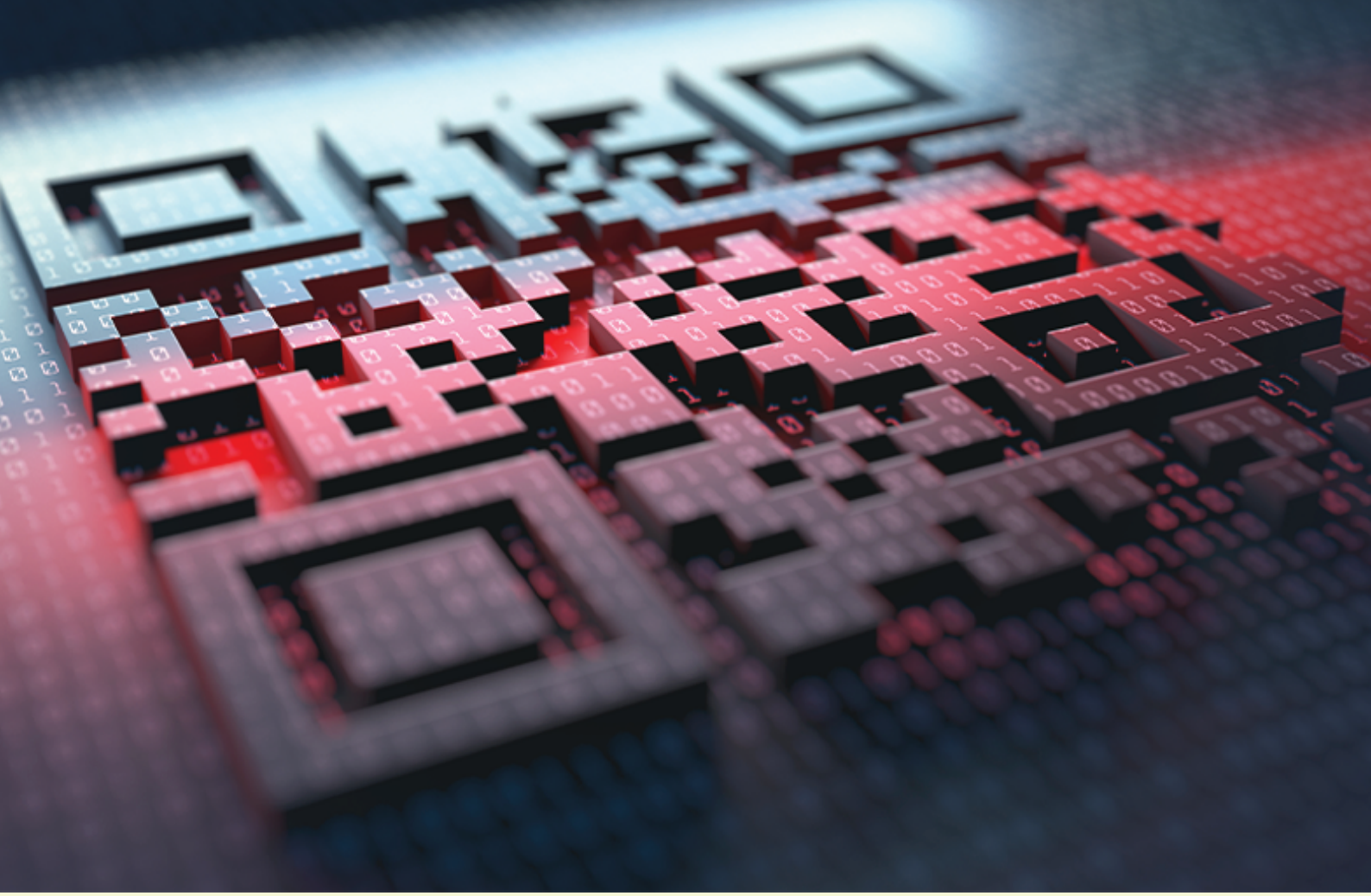
VirtuallySafe

QR CODE PHISHING OR QUISHING?

Virtually Safe | IMPACT AMPLIFIER | TEENS CAN CODE



As part of our efforts in promoting cybersecurity awareness, we want to bring to the attention of tthe public a growing threat known as QR code phishing or quishing.

You're likely not to have heard of it before, so read to the end.

WHAT IS QR CODE PHISHING (UISHING)?

QR code phishing, or quishing, is a deceptive tactic where cybercriminals use QR codes to trick individuals into revealing sensitive information, such as login, personal details, or even financial information by posing as a trustworthy entity through fraudulent emails, websites, or messages. These QR codes can be on various mediums, including emails, posters, flyers, or websites. It is a type of identity theft.

HOW DOES IT WORK?

Cybercriminals usually create malicious QR codes that, when scanned, redirect users to fake websites or applications that closely resemble legitimate ones. Unsuspecting victims may unknowingly enter their confidential information, which is then harvested by the attackers and used to harm them. A lot of institutions and organizations now work with QR codes for various purposes and projects, to make transactions and communication easier.

Some common examples or how QR codes are used include:

1. Retailers: Retail stores use QR codes for product information, promotions, and mobile payments.

2. Restaurants: Many restaurants use QR codes for contactless menus, allowing customers to view menus on their smartphones.

3. Marketing and Advertising: Marketers use QR codes to link to websites, videos, or promotions for products and services.

4. Event Management: Event organizers use QR codes for ticketing, registration, and contactless check-ins.

5. Healthcare: QR codes are used in the healthcare industry for patientv information, medical records, and prescription details.

6. Transportation: Airlines and public transportation use QR codes for mobile boarding passes and ticketing.

VirtuallySafe

7. Real Estate: QR codes on property listings provide quick access to additional information and virtual tours.

8. Education: Educational institutions use QR codes for access to online resources and course materials.

9. Manufacturing: QR codes are used for inventory management, quality control, and product tracking.

10. Logistics: Companies use QR codes for tracking packages and managing supply chains.

11. Religious organizations: Some churches and religious organizations also use QR codes as a convenient and contactless way for their members to make offerings or donations. This allows parishioners to make financial contributions using their smartphones or other digital devices. QR codes can be displayed on church websites, in physical materials, or even during religious services, and when scanned, they direct the donor to a secure payment platform or donation page. It's a modern and efficient way for churches to collect contributions and support their activities.

This, like any other well meaning tech innovation, has become a market ground for scammers. That is why it is important to adequately educate members to ensure they aren't using the wrong QR codes.

While it's relatively rare, scammers can potentially manipulate the use of QR codes in church donations. They might create fraudulent QR codes that lead to their own payment platforms or websites, diverting funds away from the intended recipients. To minimize this risk, churches and religious organizations should take precautions.

These are just a few examples, but QR codes have a wide range of applications across industries for enhancing user experiences, improving efficiency, and providing easy access to information or services.

HOW TO PROTECT YOURSELF AGAINST QR CODE PHISHING:

VirtuallySafe

1. Be Cautious: Treat QR codes with the same level of caution as you would with links or attachments in emails. Don't scan QR codes from unverified sources.

2. Verify the Source: Ensure that the QR code comes from a trusted and official source. If you receive a QR code via email or other means, doubt-check its legitimacy.

3. Inspect URLs: Before entering any information, inspect the URL displayed after scanning the QR code. Make sure it matches the official website's URL.

4. Stay Informed: Keep yourself updated about current phishing threats and security best practices. Follow us or visit our website (www.virtuallysafe.org) for more security awareness training.

5.Report Suspicious Activity: If you suspect a QR code might be part of a phishing attempt, report it to appropriate authorities immediately.

For organizations that use codes to collect funds and sensitive information from their members or public, it is important to do the following in order to keep users safe, and secure organization's funds:

1. Use a trusted payment service: Ensure that the payment or donation platform used with QR codes is reputable and secure.

2. Authenticate sources: Only use QR codes from known, trusted sources like the official church website or printed materials distributed by the church.

3. Educate members: Inform the congregation about the legitimate QR codes used for donations and how to recognize them.

4. Verify donations: Regularly monitor donations and verify that they are going to the intended church accounts.

Your cyber safety is your responsibility and our nation’s cybersecurity is a shared responsibility. Staying vigilant is crucial in protecting our sensitive information. If you have any questions or concerns about QR code phishing or any other security-related matters, please don't hesitate to reach out to us.