frogworks
Managing Your Technology So Your Business Doesn't Croak.
January 2025
01 Volume 15

Ribb"IT" Review

INSIDE THIS ISSUE:

Staying Ahead of Phishing Threats

In this always-evolving digital era, business owners have more to worry about than retaining customers and observing market trends. Cybercriminals regularly search for program vulnerabilities to exploit and override poor security systems. Still, these are far from the only threats. Many believe phishing isn't as dangerous if you can pinpoint it, but identifying it is harder than ever before.

The Traditional Method of Remaining Alert of Phishing Threats

Phishing includes sending emails or other fraudulent messages imitating a legitimate company. The scammers ask for personal data like credit card information, login credentials, addresses, and names. If the targeted team reveals this data, the attackers hold it for ransom, steal funds, or undergo identity theft attempts to ruin the company's reputation.

Traditionally, business owners encourage employees to examine all messages for misspellings that hint at fraudulent messages and email scams. Business owners also warn workers to be wary of emails:

- That ask for immediate action
- With suspicious attachments

That come from unknown email addresses

Cont. On Page 2 .

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

Staying Ahead of Phishing Threats

Cont. From Page 1.

Evolving Phishing Threats Need New Solutions

Unfortunately, as artificial intelligence and machine learning become more advanced, hackers find ways to utilize them as much as businesses and organizations. For instance, ChatGPT is a chatbot that OpenAI produced to create content and answer customer questions. However, it also deceives individuals.

ChatGPT creates realistic texts that look like they come from banks or other legitimate sources or phone scripts that imitate customer service representatives. Because it's more believable, businesses are more inclined to fall for these phishing attacks.

Quishing is another example of cyber fraud that uses a QR code rather than a traditional link during phishing attempts. When individuals click on them, they lead them to a faux login page, but unlike before, these codes don't just show up in emails. Attackers place them on social media posts, printed flyers, and in physical locations like restaurants, making them seem more trustworthy.

In addition, many scammers use social engineering to convince them to send sensitive information. For example, someone may get a notice that they must act quickly to restore stolen data, leading to them panicking and sending sensitive information.

What Your Business Can Do To Stay Ahead of Evolving Attacks

As hackers up their game, so should you to protect your business, employees, and customers. The Zero-Trust approach is an architecture that does not trust any entity within or outside the network. By default, it assumes everyone is a threat to prevent granting access to the wrong individuals, regularly asking for verification even after someone has logged in.

Even after granting access, it remains on alert, limiting access to anything outside the person's role. It also segments the network so a breach in one section won't jeopardize the company. You can also:

- Implement multi-factor authentication so hackers cannot gain company access, even with login credentials
- Use AI-powered filters and threat intelligence to pinpoint concerns
- Improve employee awareness and training with interactive modules, quizzes, and simulations

Phishing is always prevalent in our digital world. But with the right techniques and security, you can keep your company from becoming a statistic.

QR Codes Exploited to Bypass MFA Protections

Quick response, or QR codes, are ubiquitous. Businesses use them for everything from contactless access to restaurant menus and user manuals to providing payment and shopping links, making it easy for customers to access digital resources on their mobile devices. However, these codes have also created a growing security threat to businesses, as cybercriminals can use them to bypass multifactor authentication protocols and steal login credentials. Hackers launch so-called "quishing" attacks by connecting users to a website that impersonates a legitimate login page when they scan the code on their mobile device.

How Quishing Attacks Work

Exploiting QR codes for phishing is effective for one key reason: they exploit users' trust in digital scanning and barcode technology. For the average person, scanning a code in a cafe doesn't present any risk, and most of us do it regularly without any issues.

This widespread trust makes it easier for hackers to exploit the codes for nefarious purposes. A recent attack on cybersecurity firm Sophos illustrates exactly how these attacks work.

Hackers embed the codes in seemingly innocuous emails, usually appearing to come from an internal email address. When the recipient scanned the code related to employee benefits, it directed them to a malicious site designed to look like a legitimate login page. Almost immediately after they entered their login credentials and MFA token, the hackers attempted to access a secure internal application.

The network settings thwarted the Sophos attack almost immediately. However, the incident highlighted potential dangers in this form of mobile interaction

QR Codes Make It Easy for Hackers To Evade Detection

Quishing marks an evolution in phishing, making it much easier for hackers to get around email security tools designed to stop phishing attacks.

Email security filters typically filter messages with suspicious URLs, keeping them out of employee inboxes. QR codes, by default, hide URLs so the messages can slip through and reach their intended targets. When combined with other proven phishing tactics, such as social engineering, appealing to urgency and emotion, and abusing trusted domains, there's a greater chance that the recipient will respond and inadvertently expose their credentials.

QR Codes Exploited to Bypass MFA Protections

Can You Avoid Quishing Attacks?

In some ways, it's easier to avoid falling victim to a quishing attack than other cyberattacks: you won't have any trouble if you don't scan the code in the email.

That said, it's still important to follow a few best practices, including:

- Implementing endpoint security, which will catch malicious URLs hidden in QR codes
- Ongoing education about identifying phishing messages
- Confirming the message with the purported sender
- Checking the legitimacy of the URL embedded in the code, especially when it asks for sensitive data

If your company relies on QR codes to connect to digital resources, implement code encryption technology to ensure it doesn't fall into the wrong hands and become a weapon hackers can use against you.

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter