frogworks

November 2024

Issue 11 Volume 14

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

Don't Fall Victim: Protecting Your Business from Malicious Web App Downloads

Progressive web applications are valuable for business owners. These tools allow your customers or employees to view and navigate your brand's online pages more easily than traditional apps. PWAs enhance the user experience by resizing and reformatting data for mobile friendliness, which is why they're popular among top brands like Spotify or even Starbucks. But there's a catch—malicious web app downloads are everywhere now.

Your business should know about malicious PWAs and your available defenses.

How Do Harmful PWAs Work?

Many business owners consider PWAs superior to regular applications, and the installation process is similar. Users must download the app online or in locations like the Google Play store. After the installation, a shortcut becomes available for your customer to access that app.

From there, PWAs differ from traditional apps. Clicking on a PWA opens the user's web browser (not the app). Unfortunately, since search engines are filled with faux websites and applications, a plethora of malware might be what your clicked link finds instead.

Have your customers or employees downloaded a malicious PWA that looks exactly like your business' original one? If so, clicking on it will open their browser page and lead them to one of these fake sites. These convincing programs harvest data and steal credentials, like passwords and credit card numbers, so the potential fallout for your business is, frankly, terrifying.

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

Don't Fall Victim: Protecting Your Business from Malicious Web App Downloads

How Can You Protect Your Business From PWA Cyberthreats?

Your business would much rather forgo the theft, slandering, and revenue hit of customers who no longer trust your brand. So, how can you protect your operation from real threats online, like this malicious code?

Don't Ignore Abnormalities

One cybersecurity professional, Mr.d0x, described this malware from his research efforts that released GitHub phishing templates. This research confirmed that PWA amateurs are likely to become victims because of a lack of awareness. For example, PWAs should always have a URL bar.

Business owners can train employees to recognize these types of PWA abnormalities. Do they know what differentiates real and faux PWAs? Do they double-check URL addresses for misspellings or extra or missing letters when downloading the app?

Track Non-Company Users

Suppose hackers that create malicious web app downloads receive the credentials they need to breach your company. Can they steal more personal information? Your business will want to learn about these attempts before they do.

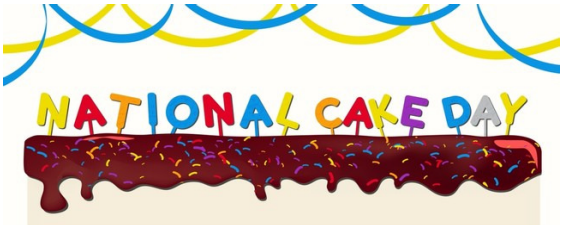
Monitor third-party activity in your database or operating system from an external source. By restricting third-party access to sensitive data, you can halt breaches.

Never Delay Security Updates

Has a faux party application tried to access your customer or employee's information? The latest security updates can protect your system against malware, including:

- Downloading the most recent iOS to obtain patches for any security leaks.
- Updating anti-virus and anti-malware regularly to alert you to suspicious files.

Your business's best offense is a good defense, so keep those malicious web app downloads out of the office!



November 26th

Securing Your Business With Multi-Factor Authentication

Most people expect to enter a username and password to access secure networks and accounts online. They also expect that password protection for sensitive data will stop unauthorized access.

Unfortunately, single-factor authentication is no longer enough to fully secure your business networks and resources. Password theft is one of the leading causes of data breaches, with hackers using stolen credentials to access sensitive information and wreak havoc on businesses. However, by taking a multi-layered approach to cyber security that uses multi-factor authentication, you stand a better chance of thwarting bad actors and keeping your business data safe.

What Is Multi-Factor Authentication?

The typical username and password combination that we're all familiar with is a type of single-factor authentication. In order to access a protected asset, you only need a single factor (in this case, the password) to prove you have permission to do so.

Multi-factor authentication requires several pieces of information for user verification. In most cases, these include the username and password, as well as another token, like a unique code. These additional authentication factors help ensure that even in the event of a password compromise, whoever has the password won't be able to go any further because they don't have the additional details.

Authentication factors can come in a variety of forms, including:

- **Biometrics,** such as a fingerprint or facial recognition
- **Mobile apps** that continuously generate one-time passwords to enter in addition to your standard username and password
- **SMS texts**, which deliver a one-time code to a mobile device
- **Hardware tokens**, which are physical devices that generate one-time codes or that you insert into a device in addition to a password

Security questions that the user establishes at account setup

Securing Your Business With Multi-Factor Authentication

Why You Need Multiple Security Layers

Ultimately, implementing several security layers helps reduce the risk of many common cyber threats that can cost your business time and money. Considering that many small and midsize businesses never fully recover from a cyber attack, investing in multi-factor authentication is an important element of a robust approach to security.

Using multi-factor authentication offers several major advantages.

Increased Protection

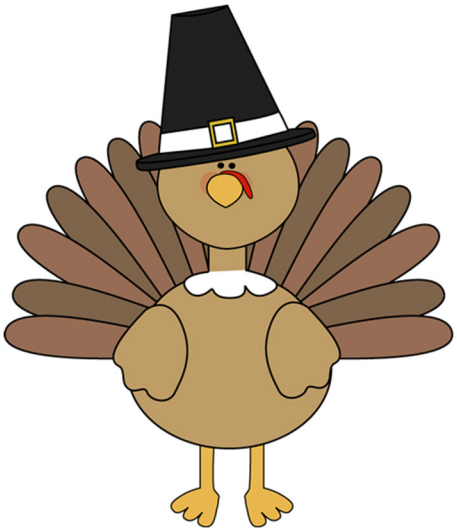
Even if you run a small business, there's always a threat of attack. Hackers use a variety of methods to steal passwords, like brute force attacks, social engineering, and date packet sniffing, but if you have multi-factor authentication in place, simply getting those passwords isn't enough to get into your network.

Requiring additional information before granting access to sensitive assets allows your cyber security team to focus on other priorities. It's just one tool of many that they can use to address the barrage of threats coming from every direction.

Simplicity

Using this type of security is easy. It takes the typical user only a few seconds to generate and enter a code. Considering the many hours it takes to respond to a data breach, not to mention the impact that one will have on your business's reputation and bottom line, there's really no comparison.

Cyber threats are always evolving, but multi-factor authentication is a simple and effective way to proactively protect your business.



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