frogworks

August 2025

Issue 08 Volume 15

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

Secure Passwords Without Sacrificing User Experience

Cybersecurity is a priority for businesses, but the reality is that most of your employees will choose convenience over security every time. In other words, if they see security measures as a hassle when logging in to their email or other accounts, they'll take shortcuts like using weak passwords, reusing old ones, writing them down, or never logging out. They can get into their accounts faster, but they put your company at risk for devastating cyberattacks.

Solving this problem doesn't mean choosing between strong security and a seamless user experience (UX). With the right approach, you can have both.

Why Security vs. UX Feels Like an Unwinnable Battle

There's no question you want to protect sensitive data, but when complex security measures frustrate users, they will find a less secure alternative to getting where they need to be.

The result? People develop bad habits, like writing down their credentials or using the same credentials everywhere. The problem isn't just internal; if your vendors make logging into SaaS or other platforms feel like a chore, your employees might turn to easier, unauthorized alternatives that are riskier to use.

The challenge is clear: How do you secure passwords without making users jump through hoops? The answer lies in innovative, user-friendly security strategies.

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

Secure Passwords Without Sacrificing User Experience

5 Smart Ways To Balance Security and Login Convenience

1. Adopt Password Managers
Expecting users to create and remember unique passwords for every account is unrealistic. A password manager is a better solution. These tools generate and store strong passwords, so users don't have to.

2. Leverage Multi-Factor Authentication (MFA) Wisely
Multi-factor authentication (MFA) effectively protects accounts but can feel like an extra burden for users. The trick is to use it strategically. Adaptive authentication, where extra verification is required only when a login attempt seems suspicious, keeps security tight without annoying users unnecessarily.

3. Use Passkeys and Biometric Authentication
Passkeys, which use cryptographic authentication instead of traditional passwords, are gaining traction as an alternative to conventional username and password combinations. Biometric verification options like fingerprints, facial recognition, and behavioral biometrics also offer frictionless yet secure passwordless authentication.

4. Set Smart Password Policies
When a platform requires a password, don't complicate the requirements. Instead of forcing frequent password changes (which leads to weaker passwords), focus on longer passphrases that employees will remember but hackers can't crack.

5. Reduce Login Headaches With Single Sign-On (SSO)
Single Sign-On (SSO) lets users log in once and access multiple systems. This approach minimizes password fatigue while maintaining strong security controls. It improves UX without compromising protection.

Security and UX Can Coexist With Password Alternatives

Implementing user-friendly security measures like password managers, adaptive authentication, passkeys, and SSO keeps your company's accounts safe without frustrating users and driving them to less secure passwords and solutions. The key is to make security effortless because when security feels easy, users are far more likely to embrace it.

Is Your Smartphone a Cybersecurity Risk?

Is your smartphone a cybersecurity risk for your business? It's easy to overlook how much confidential information lives on your device.

Hackers know this, and they're targeting mobile phones more than ever. Keep reading to learn more.

Everyday Reliance, Everyday Risk: The Smartphone Dilemma

Our phones are with us all the time, both at home and on the go. They help us stay connected, manage tasks, and access data instantly.

For business owners, they're even more critical. Everything happens through these small devices, from checking emails to handling payments.

Unfortunately, the risks to personal identity and cybersecurity continue to escalate. Let's go over some major incidents so you can better understand the gravity of the situation:

- **AT&T breach**: Cybercriminals extracted the metadata texts and calls from nearly all of AT&T's cellular customers. The content of the communication remained secure, but it has raised privacy concerns.

National Public Data breach: Hackers leaked the personal data of almost 3 billion individuals on the dark web, which included names, addresses, and Social Security numbers.

What Are the Emerging Dangers for Mobile Devices?

Is your smartphone a cybersecurity risk? Watch out for these common threats:

- **Mobile malware**: Dubious websites, apps, and links can inject malicious software into your device and compromise sensitive data.
- **Phishing attacks**: Fake emails and messages trick you into revealing personal information.
- **Public Wi-Fi risks**: Unsecured public networks are a playground for hackers.
- **SIM swapping**: Sophisticated scams can fool providers into transferring your number, giving hackers access to accounts that require phone verification.

IoT vulnerabilities: Smartwatches, fitness trackers, smart speakers, and other devices connected to your phone create additional entry points for attackers.

Is Your Smartphone a Cybersecurity Risk?

Keeping Your Mobile Device and Data Safe

The last thing you want is a phone data breach that ruins your establishment's reputation. Consider these simple but effective tips:

- **Strengthen login credentials**: Create strong, unique passwords for every account, and use a password manager to track them easily. Enable two-factor authentication whenever possible, too.
- **Back up your data**: Use cloud storage or external drives so you don't lose everything when something happens.
- **Update your software often**: Outdated systems can leave your business vulnerable. Install app and operating system updates promptly to patch security flaws.
- **Think before you click**: It's always wise to pause and verify links or attachments in emails, especially when they seem unexpected or too good to be true.
- **Improve app security**: Only install applications from trusted sources and limit app permissions. The permissions you grant should align with the app's purpose.

Avoid connecting to public networks: Use a reliable VPN to protect your personal information online. Never use public Wi-Fi for sensitive tasks like banking or shopping.

Is your smartphone a cybersecurity risk? These devices boost business productivity by enabling instant communication, remote work, and on-the-go access to tools, but they also carry risks. Familiarize yourself with the latest smartphone vulnerabilities, stay on top of operating system updates, and take other proactive steps.

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