July 2025
Issue 07 Volume 15

frogworks

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

Scammers Are Posing as Microsoft and Google

Could you or your staff reliably spot a scam disguised as a legitimate message? Scammers are getting smarter and targeting establishments just like yours. Keep reading to learn more.

How Recognized Brands Are Becoming a Threat Actor's Best Tool

Have you noticed how certain brands instantly make you feel at ease? Many industry giants dominate our daily operations and build trust effortlessly — cybercriminals know this and use familiarity to craft sophisticated phishing attacks.

Watch out for emails or messages from Microsoft in particular. A study by Check Point shows that scammers impersonate this brand the most, making up 36% of observed brand-related social engineering attacks in 2025's first quarter. Google and Apple follow behind at 12% and 8%, respectively.

This means over half of all identified attacks (56%) have posed as one of these three brands.

Mastercard Users Beware

There's also a recent spike in cybercriminals impersonating Mastercard. Fraudulent campaigns have targeted mostly Japanese users through fake login pages.

These websites mimic genuine platforms and trick people into sharing card numbers, CVVs, and other sensitive financial details. Always verify website URLs, and it never hurts to contact customer support when any doubt remains.

Get More Free Tips, Tools, and Services At Our Web Site: www.GetFrogworks.com
Or call: (240) 880-1944

Scammers Are Posing as Microsoft and Google

What Exactly Are Phishing Attacks?

Phishing is a type of cyberattack that tricks you into giving away sensitive information. For example, scammers might pose as a bank representative or supplier and ask for payment on a fake invoice.

Another common tactic is sending links to carefully crafted websites. Any login details entered there could be stolen.

How To Defend Your Business Against Branded Phishing Attacks

Why wait for your company to become a target? Follow these steps to minimize risks:

Employ Anti-Phishing Measures

Even the most vigilant individuals can still occasionally fall victim to sophisticated attacks. Modern technology can pick up the slack. Common software solutions include:

- Filters that automatically remove phishing email impersonation messages or deceptive requests

- Integrated anti-malware that scans incoming emails and attachments

Link analyzers that prevent users from engaging with potentially harmful links

Strengthen Cyber Awareness Across Your Organization

Train your team to recognize fake email addresses, suspicious links, and unsolicited requests. Drill the importance of using strong passwords, avoiding public Wi-Fi for sensitive work, and reporting unusual events.

It's also worth creating workshops and phishing simulations to help keep everyone sharp. Practical sessions build confidence and reduce mistakes.

Create Incident Response and Recovery Plans

What if your team falls for a tech support scam or Microsoft impersonation fraud? The most successful companies have clear steps in place when the worst happens.

An effective response plan includes clear roles, quick communication, and real-time detection. Focus on isolating threats, mitigating damage, and restoring systems. Regularly update your plan, train your team, and create secure backups for smooth recovery.

Securing Your Establishment's Future With Preparedness

Don't wait until a Google account scam or similar threats disrupt operations. Scammers are evolving fast and use smarter tactics every day.

Business owners must stay alert and proactive. Protect your digital assets, educate your team, and update defenses regularly.

Businesses Still Use Weak Passwords — And It’s a Huge Risk

Can you imagine spending years building your business, only to have it compromised in seconds because you decided to use “password” as your login code? You might be thinking, “Who would do that?”

According to research from password manager NordPass, more people than you might expect are using weak passwords, putting their businesses and livelihoods at risk. So why are people still using easily guessable passwords at work?

The Ugly Truth About Passwords

If you use a password like “qwerty” or “123456,” a hacker could crack it before you finish reading this sentence.

Weak passwords make a hacker’s job easy. Criminals don’t have to do much to get into your company’s network or accounts. Once they do, they can steal sensitive data and financial information or even take control of entire business systems.

The effects of such a break are costly to any business. Still, a single breach can tank the entire company for small and medium-sized enterprises. According to Verizon, as many as 60% of small businesses never recover from financial losses, reputational damage, and legal trouble caused by a breach.

It’s not just weak or easily guessable passwords that cause problems, either. Using a default or identical password for numerous accounts is also a problem. It leads to credential stuffing, in which hackers use the usernames and passwords stolen from one service to attempt to log in to others.

Forbes Advisor reports that 78% of people use the same credentials for an average of four services. Most cite convenience as the reason for reuse; they don’t want to create and remember complex logins for dozens of accounts.

Another issue is that many people don’t know how to create a solid password. The best passwords are complex, with at least 12 characters and a mix of symbols, numbers, and letters.

These ideal passwords can be hard to remember, though. To make things easier, people use common dictionary words instead. But this only puts them at risk for dictionary attacks, in which hackers systematically enter every word on a list to figure out the password.

Businesses Still Use Weak Passwords — And It's a Huge Risk

How To Solve the Password Problem (Without Losing Your Mind)

Protecting your business with strong passwords doesn't have to be complicated. Starting with a strict password policy, you can implement simple protocols and tools to avoid a password-related breach.

Other ways to keep passwords secure include:

- Enabling multi-factor authentication (MFA) so that even if a hacker gets your password, they must complete a second verification step to gain access.

Changing default passwords on business tools and software immediately.

Passwords Should Be Secure — Keep Them That Way

Weak passwords could be all hackers need to walk through your business's front door and cause catastrophic damage. Take action today to strengthen your passwords and keep your business safe.

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