frogworks

June 2025

Issue 06 Volume 15

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

OneDrive for Business May Not Be Fully Secure

Heads up: If your company uses OneDrive for Business to store critical documents in the cloud, they may not be as secure as you think.

According to security expert Brian Maloney, Microsoft is not adequately securing data on user's devices, which could present a massive security risk if that device becomes compromised. Without adequate OneDrive for Business security, sensitive information could easily fall into an attacker's hands and have consequences for your company.

What Businesses Need To Know About the OneDrive Data Vulnerability

The Microsoft OneDrive risks stem from an issue with Optical Character Recognition (OCR), a tool that supports search functions. When you search your files in your OneDrive account, the system automatically saves the OCR data as a plain text image in a database on your computer. Additional security experts also note that pictures saved with OneDrive are stored in an unsecured SQLite file.

Why is this an issue?

The problem isn't necessarily as much of a concern when your team works on company-issued hardware, as those devices typically have multiple layers of security in place. OneDrive for Business Security concerns arise when employees use their devices to access their OneDrive accounts. When they access files on devices that don't have the same level of data protection, OneDrive files become more easily accessible.

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

OneDrive for Business May Not Be Fully Secure

Cloud Storage Security Tips To Protect Your Business

Because Microsoft has not acknowledged this issue or explained why it doesn't secure OCR databases, it's up to you to implement business cloud security measures to protect your company from the risk of a data breach.

Some of the ways you can protect your company and bolster OneDrive for Business security include:

- Implementing network access control (NAC) to block devices that don't meet your security standards from accessing your company network
- Requiring employees to use a VPN for any work-related tasks on their own or company-issued devices
- Managing OneDrive Access Controls appropriately to restrict access to the most sensitive data to authorized individuals
- Maintaining a comprehensive updating and patching protocol that ensures Microsoft 365 and OneDrive always have the most up-to-date security protections in place
- Using two-factor authentication and strong passwords

Disabling One Drive features that you won't use to reduce risk

Although these cloud security tips can help protect your OneDrive for Business account, they aren't foolproof, especially since the major issue is the potential for sensitive information on your employee's devices. With that in mind, you need to consider whether you'll allow your team to use their own devices for work and, if so, whether they'll need to meet specific security standards.

It's also important to reiterate to your employees that they must be as vigilant when using their devices as they are at work. Phishing messages can land in their inboxes at home, too, and their internet habits could create security risks. Staying alert to risks 24/7 can help protect your company from the fallout of a OneDrive for Business security breach.

Hackers Exploit Victims with Scam-Yourself Attacks

Recent research from GetApp shows that over 81% of people open phishing emails on their work devices.

One big reason for this issue is that many hackers exploit victims with scam-yourself attacks. That's right: With the right amount of psychological manipulation, hackers can trick almost anyone into falling for their phishing attacks.

How Can You Scam Yourself?

According to a threat intelligence report from Gen, scam-yourself attacks increased by 614% in 2024. These cyber-attacks use social engineering to manipulate people into malicious acts like malware distribution without them even realizing it. Hackers tap into basic human nature, using tactics like creating urgency or fear, impersonating real people or organizations, appealing to curiosity, pulling on victims' heartstrings, or targeting greed.

Whatever approach they take, when hackers exploit victims with scam-yourself attacks, they can gain access to your business's sensitive information, steal money, and generally wreak havoc on operations.

How People Are Scamming Themselves

In 2024, several attacks significantly increased, turning normally vigilant people into victims. These schemes compromised corporate and personal data and banking information, launched ransomware attacks, and more.

ClickFix

ClickFix scams target individuals having issues with their devices. When they look for solutions, malicious sites present fake solutions, typically copying and pasting malicious code into command prompts. Instead of solving the problem, the code grants hackers total control of the device and access to all its data.

Hackers Exploit Victims with Scam-Yourself Attacks

Fake Software Updates

Fake updates are malware disguised as harmless but urgent updates that you must install immediately to keep your computer or software working.

Fake CAPTCHA

We've all had to click a button or solve a puzzle to prove that we're not robots online, and hackers have found a way to create fake CAPTCHAS for malware distribution. The scheme tricks people into solving an "I'm not a robot" puzzle, which causes victims to copy malicious code and infect their devices.

Keep Your Business Safe From These Attacks

Given that so many people encounter phishing at work, businesses have to take steps to secure their networks. Knowing that hackers exploit victims with scam-yourself attacks, it's important to develop policies regarding downloads, software updates, and technical support that prohibit employees from being able to use unapproved sources. Other effective tactics include:

- Limiting administrator privileges so users can't install anything without approval.
- Implement advanced threat detection and malware-blocking tools to stop attacks in their tracks.
- Regularly updating operating systems to block common exploits.

It's hard to overcome human nature when protecting your business, but staying vigilant to threats can go a long way toward preventing a breach.

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