frogworks

Managing Your Technology So Your Business Doesn't Croak.

2023

Issue 10 Volume 13

Ribb"IT" Review

INSIDE THIS ISSUE:

Hackers Can Fool Multi-Factor Authentication

In the world of cybersecurity, change is the only constant. For many business owners, multi-factor authentication (MFA) has been the go-to option for extra security. But hackers today are more ingenious, working around the old systems that used to stop them. New tricks are emerging to get business data and customers' sensitive information. MFA remains an essential to online security, but hackers are figuring out ways to bypass it.

Why Does This Matter for Your Business?

The danger is that hackers could take over your business account. Hackers who get past your MFA could get to your private business data. They could mess up your work, misuse your customer data, or even conduct fraud under your name. Just using MFA isn't enough anymore.

MFA Weak Points

Here are possible vulnerabilities in the MFA system that businesses should know:

Social Engineering. Hackers trick users into giving away their MFA codes by pretending to be someone they trust, like customer service or IT support.

MFA Prompt Bombing. Hackers will send too many security requests, so you click "approve" to stop the alerts. Once you do, the hacker, who started the prompts, gets access. (see page 2)

Stealing Codes. Threat actors steal your password or security code by intercepting your messages with the security team.

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

Hackers Fool Multi-Factor Authentication (cont)

More MFA Weak Points:

- **MFA Prompt Bombing.** Hackers will send too many security requests, so you click "approve" to stop the alerts. Once you do, the hacker, who started the prompts, gets access.

- **SIM Card Swapping.** This happens when a hacker fools your phone company into giving your phone number to their SIM card. They can then steal security codes sent by text.

- **Malware.** Threat actors can use harmful software to get to your device and steal MFA data through bad apps, email attachments, or unsafe websites.

Strengthening Your MFA Strategy

Rethink how you manage your online security by enhancing password hygiene and promoting a culture of alertness. Use different, tough-to-guess passwords for more secure processes. Train your team to recognize when someone is trying to steal their info. Educate them about the latest tricks used by hackers. Keep your systems and security software updated. Updates often include fixes for new threats. In addition, consider using controls that limit unsuccessful login attempts. This can stop attacks and protect against account lockouts.

A Layered Defense Is Your Best Offense

MFA is an integral part of your strategy to stay safe online. However, it shouldn't be your only security strategy. Knowing how hackers get past extra security and staying informed about new cyber threats helps you protect your business. Create a robust security system with many layers. Ultimately, it is all about staying one step ahead of the hackers.

Tech-Related Risks Businesses Need to Consider

As businesses use digital solutions, business owners and CEOs need to be aware of the possible risks of the tech they've chosen. Even though many solutions have good security features to protect their customers, you should still look at specific risks and how likely they will affect your business. Here are five chances that companies need to think about when it comes to technology.

You already know about some of the risks that come with technology. Remember these risks to protect your business and deal with possible threats cautiously. (see page 3)

Tech-Related Risks Businesses Need to Consider (cont)

1. Accountability

First and foremost, businesses should have a team that works to reduce risks and takes responsibility for any mistakes. This group should develop new ways to protect the business's digital assets. It should also help hold people accountable if a big problem comes up by:

- Figuring out what caused the problem
- Assisting with drafting public statements about the issue

Finding and sharing solutions that address the problem

2. Data Loss or Breach

Even with advanced security steps, your business can still lose or steal data. Personal or financial data saved on a company's cloud is a clear example of data people want. One data source that is often overlooked is the technology you use to run and organize your business.

If you protect your business's mindset, knowledge, and methods, that critical information might not reach competitors. Some of the best ways to run a business are to keep trade secrets secret and to keep customer and staff information safe.

3. Technical Debt

Many business owners don't worry about technical debt. Any debt resolution is a long-term goal to achieve. Still, prompt resolution leads to more success in the immediate future. See whether your team can resolve any issues with your current digital infrastructure each month. This allows your staff and customers to quickly adapt to and appreciate the changes while progressing your company.

Tech-Related Risks Businesses Need to Consider (cont)

4. Personal Device Usage

Everyone owns a mobile device these days. You'll commonly see customers and employees alike check their phones or tablets occasionally. But personal devices only sometimes sport the most recent security features necessary to prevent malware and other threats from attacking your network.

Look into implementing risk management policies that address this. You can also install a guest network for device connections.

5. Phishing

Phishing is among the oldest tech-related risks businesses need to consider. Yet, many staff members can still fall for a phisher's sophisticated tricks. Phishing attempts are not as obvious as they once were. A phishing email can perfectly reflect a newsletter from inside the company.

Keep your staff updated about what more recent phishing emails might look like.

Newsletter Word Search

```
U I D J F R O G W O R K S M A
L O J J O Q D H I E H N Q B E
Y M X N Q Q B M D I C E T K H
K U F V R L Z E Y R Z W N T U
D A Y P Z G T B X Y J S P G Q
P L C X H B Q W A Y T L I Y H
T E K O Z I K L I Z F E D I Q
C X B W M O S T W F W T I S B
K L L D P P W H Y U I T N A R
W L L J G P U I I N W E T I E
I J D Z E O T T A N S R E A A
D O E U I Z J D E D G D R H C
N E T Q L D C B D R Y M N Q H
C Y L F K I J Z G Y S Q E F D
X Q I M A L W A R E B I T R S
```

Newsletter	Frogworks	Computers	Alex
Phishing	Internet	Malware	Wifi
Breach	Isaiah	Joey	

Strong Risk Management for Businesses

Stay updated on these and other tech-related risks businesses need to consider. Doing so will protect your business currently and in the future. Learn more proactive approaches to risk management.

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

Channel Futures
Leading Channel Partners Forward
NEXTGEN 101
MSP TO WATCH • 2021 WINNER