2024
Issue 8 Volume 14

frogworks

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

How Identity Theft Affects Small Businesses

As a small business owner, you may assume that larger businesses are at a greater risk of hackers stealing their data. Don't big companies have more revenue and sensitive information at stake? While that might be true in one sense, sources like Insurance Business say that, in general, cybercriminals are more likely to attack small businesses since they have fewer security measures in place than corporations.

Let's look at the impact of identity theft on small businesses.

What Is Identity Theft Online?

Like non-digital identity theft, an online hacker will get information from your small business or its employees and pretend to be you. Countless hacking techniques steal your social security number, passwords, and other personal or financial information, including:

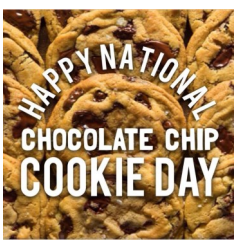
- Phishing, which sends you to faux websites

Viruses, which enter your network and deliver stored data directly to hackers

How Can Identity Theft Harm Your Business?

After accessing and using personal data, the thief conceals their identity until they finish cashing out as much as possible. They then close the account to avoid detection. In the process, your business can lose a lot: money, reputation, trade secrets, and much more.

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



How Identity Theft Affects Small Businesses

Loss of Finances

The most obvious identity theft problem is losing funds to a mysterious third party with unauthorized access to your business network. They can steal enough so that your operating expenses outweigh your revenue, tanking your operations.

You'll also have to spend money to undo these damages, including compensating employees and customers or even regulatory fines.

Legal Issues

Recovering from identity theft is hard if regulatory bodies do not take your compromised customer data lightly. They fine you for your ineffective security system in terms of the laws meant to increase privacy.

It's a loss of finances, making your company less safe and reliable. You'll lose customers.

Tainted Reputation

What happens with diminished customer trust in your small business? Nothing good.

Suppose one or more customers find their information compromised, and word gets out. In that case, your business would look like those scammer websites.

Sometimes, it takes years or even decades to rebuild that trust. Could your business give up and rebrand? You won't have to work your way from the ground up with the right proactive measures to prevent identity theft.

Prevent Loss With the Right Measures For Your Business

Pay attention when you notice signs of identity theft, such as unauthorized credit card purchases or fraudulent tax returns. The following practices may keep your credit score up and any police report at bay:

- Use strong passwords (letters, numbers, symbols, and multi-step authentication).
- Do not click suspicious links.
- Teach employees the warning signs of online scammers
- Don't wait to report unusual activity in your personal or business accounts or networks.
- Choose secure connections and VPNs

Identity theft is not a victimless crime. Consider the potential impact of identity theft on your small business and take the appropriate measures.

Hackers Can Now Steal Face Scans

Biometric authentication factors like facial recognition scans are no longer iron-clad cybersecurity measures. Emerging technology allows hackers to steal face scans and infiltrate a user's unauthorized accounts. Learn how these social engineering attacks take place and what you can do to protect personal data.

Flaws With Multi-Factor Authentication

Cybersecurity experts praise multi-factor authentication as a key way to protect sensitive data. Rather than just entering a username or password, you'll use one or more other credentials to verify you as the account holder. Common forms of MFA include:

- Answering security questions before logging into an account
- Entering a one-time passcode that you receive via email or text message
- Using biometric authentication like facial recognition or fingerprint scans to identify you

Savvy hackers can infiltrate accounts when you use MFA measures like personal identification numbers or security questions. Recent vulnerabilities emphasize the need for biometric data protection since threat actors are stealing sensitive data.

How Hackers Execute Facial Recognition Data Theft

All apps on your device are safe from hacking since you log in by showing your face. However, some users fall victim to identity theft because hackers learn how to steal face scans. Discover how this issue can impact you.

Cybercriminals Create Fake Apps Requiring Biometric Data

How is it possible for a hacker to steal face scans? Vulnerable users fall victim to this attack by letting a fake app led by bad actors perform a biometric scan. Hackers can access this sensitive data as soon as the scan is completed.

Hackers Can Now Steal Face Scans

AI-Powered Deepfake Creations

Groundbreaking artificial intelligence becomes a problem when hackers use this technology to create a deepfake image of people after stealing their biometric data. This replicated image allows cybercriminals to bypass sensitive biometric multi-factor authentication methods.

Users Lose Access to Secure Apps

Once a hacker completes the steps above, they can easily infiltrate apps. This cyberattack causes the most harm when threat actors receive unauthorized bank access to various financial apps. By impersonating the user, they can access bank account numbers and cause significant economic loss.

How To Protect Your Biometric Data

As a business owner, you must take steps to keep biometric data secure so hackers can't access your more sensitive accounts. Experts recommend boosting your cybersecurity measures across the board, including:

- Educating your workforce about social engineering attacks and how to spot the signs of one
- Monitoring all devices for malware and performing regular audits using endpoint protection software
- Increasing your awareness of potential threats and mitigating them with patch management

The current threat does not center around iOS and Android vulnerabilities. It is only active for users in an undisclosed region. However, taking the necessary precautions to protect yourself is wise as hackers learn new ways to steal face scans.

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

AUGUST IS HAPPINESS HAPPENS MONTH.

Share your happiness and encourage others to do the same.