May 2024
Issue 5 Volume 14

frogworks

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

The Dangers of These Social Media

Social media is a part of our everyday lives. Despite the many benefits of these platforms, social media privacy issues remain a major concern among users.

Learn about the sensitive information that social media sites can access about their users and why it's important to maintain privacy while using these sites.

Why Social Media Use Doesn't Ensure Privacy

A key part of social media is to share photos, videos, posts, and updates about one's personal life and interests. Users can decide what kind of information they voluntarily post on sites like Facebook or LinkedIn. However, personal, identifiable information is also available based on the site's privacy setting loopholes.

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

The Dangers of These Social Media Privacy Issues

Sites can release a user's information via tracking cookies and then take part in third-party data sharing. Tracking cookies will monitor key parts of someone's online activity, including:

- Websites they visit
- Keywords they search for
- Purchases they make
- Social media posts they share

Risks of Social Media Data Mining

All the information that tracking cookies collect becomes valuable for companies looking to advertise to customers. Data brokers can sell the segmented information so companies can create customized ads, which remains one of the most controversial social media privacy issues. The problem escalates when hackers and cybercriminals gain access to this information.

Threat actors can obtain sensitive user information and execute attacks on their networks. Data mining can lead to a data breach and puts users at risk of receiving malware and viruses that destroy their device's network.

Noteworthy Social Media Privacy Issues

In addition to data mining, users subject themselves to several other privacy concerns when they use social media. Below is a breakdown of key issues to be aware of as a business owner.

Location Settings

Hackers can manipulate a user's location settings to obtain more data about them. Adjusting the settings on a social media site will protect you since scammers can track your device's location through public Wi-Fi networks and cellphone towers. The best way to keep your location private is to turn off GPS location services and use the site on a virtual private network.

Fake Information

Bots and malicious actors can spread false information across social media sites. Most platforms have procedures for flagging and removing false or misleading content. It can take some time for moderators to address every post containing fake information, so remember to fact-check everything you see on social media.

Awareness of these social media privacy issues isn't enough to protect yourself. You must also take the proper

The Impact of Data Breaches on Businesses

Do you run a small business? You're probably well aware of the dangers a data breach poses to your company.

Never underestimate the impact of data breaches on businesses. Then, you can stay vigilant and protect yourself. Keep reading to learn the growing danger of these attacks, the damage you can expect if you experience one, and how to protect yourself.

The Prevalence of Data Breaches

Data breaches are among the fastest-growing business data security risks. Statista.com reported over 3,000 data breaches in 2023, compared to 1,800 attacks in 2022.

In some years, we see a marginal decrease in breaches. However, most years see an increase in both frequency and complexity.

The National Cybersecurity Alliance reports that 70% of all cyberattacks target small and medium businesses. Most can't recover from the attacks, and some small businesses shut down.

Never assume cyber attackers will ignore you or that you could recover. One of the smartest investments you can make is in cybersecurity.

The Devastating Effects of Data Breaches

The impact of data breaches on businesses can be devastating. But what are the consequences of corporate data breaches? When a hacker obtains the sensitive information of your customers or employees, you'll experience the following challenges.

Fines and Fees

The most immediate impact of data breaches on businesses is the fines and fees they will pay. These fines are imposed by regulatory organizations and government institutions created to protect consumers.

After a data breach, the Payment Card Industry Security Standards Council can impose a fine on your business. Depending on your industry, other regulatory industries may fine you as well. From the PCI SSC, the fine can include a $90 charge for each affected credit card and up to $500,000 in additional penalties.

The authorities will require you to conduct a forensic investigation. The investigation aims to determine the attack's cause and the weakness in your security. You'll pay at least $10,000 for this investigation.

After a data breach, you may become responsible for monitoring the credit of affected customers.

The Impact of Data Breaches on Businesses

Loss of Reputation

A long-lasting cybersecurity impact on companies is the loss of customer reputation. One PwC report indicates that 85% of consumers won't shop at a business if they're worried about its cybersecurity practices. Another study from Verizon shows that nearly 70% of people actively avoid businesses that have experienced a data breach.

Lost Intellectual Property

One important reason for investing in cybersecurity is safeguarding business information. This includes designs, strategies, and new products you require to grow your business. Losing your intellectual property can stop your business growth for the foreseeable future.

Protect Your Business With Cybersecurity Practices

Now that you know the impact of data breaches on businesses, you can implement proper prevention measures. You can implement several methods to avoid losing business continuity after a data breach and to prevent the breach from ever occurring.

Make sure your employees create strong passwords and can identify phishing scams. Enable two-factor authentication on all devices and applications. Invest in cyber monitoring and strong antivirus software.

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