CYBERRISKS+LIABILITIES

November/December 2018

IN THIS ISSUE

hierl

Facebook Security Breach Affects Nearly 50 Million Accounts

Recently, Facebook announced that nearly 50 million user accounts were compromised in a data breach. The breach, which can be traced back to July 2017, is one of the largest in the company's 14-year history.

While investigations are ongoing, the company said hackers exploited a software vulnerability in Facebook's "View As" feature to steal access tokens and gain control of user accounts. Access tokens are effectively digital keys to specific accounts, and stealing them allows attackers to view private posts or compose status updates without the knowledge of the affected user.

In addition, the attack allowed the hackers to see anything that users can see on their own profile, including the names and birthdates of friends and family members. Such information could be used in future phishing attacks.

In response to the attack, Facebook reset 90 million logins automatically, fixed the software vulnerability and informed law enforcement officials. While the company says that users do not need to change their passwords, individuals experiencing login issues should navigate to Facebook's Help Center.

As a safety precaution, users are encouraged to log in and out of all of their accounts on every device. Users can see all of the devices they're currently signed into here.

To learn more about the breach, read Facebook's official blog post.

5 Tips to Make Your Passwords More Secure

Because identity theft and data breaches are becoming an ever-growing problem, it's important to not only have a different password for each account, but to make those passwords easy to remember and hard to guess. The following are tips you can use to make your password harder to crack:

1. **Change your passwords every 90 days.** This might seem like a hassle at first, but hackers have a better chance at cracking your passwords if they never change. It's also a good idea to avoid reusing passwords.
2. **Make your passwords at least eight characters long.** Generally, the longer a password is, the harder it is to guess.
3. **Don't use the same password for each account.** Hackers target lower security websites and then test cracked passwords on higher security sites. Make sure each account has a different password.
4. **Include uppercase letters and special characters in your password.** Special characters include symbols like "#," "*," "+" and ">." These symbols can make your password more complex and harder to guess.
5. **Avoid using the names of spouses, kids or pets in your password.** All it takes for a hacker to crack passwords that include these things is a little research on social media sites like Facebook and Twitter.

3 Network Security Threats to Watch Out for in 2019

Cyber security attacks continue to increase in both size and severity. In order to truly protect themselves, businesses must remain informed on the latest cyber security trends. While it can be difficult to predict the emergence of new risks, the following is a list of major threats experts have identified for 2019 and ways to protect your business:

1. **Viruses and worms**—Computer viruses and worms are malicious programs designed to infect core systems and destroy essential data. What's more, viruses and worms can replicate themselves, infecting an entire network quickly. To protect your system, install anti-malware on all network devices.
2. **Drive-by download attacks**—Drive-by download attacks generally refer to the unintentional download of malicious code from an app, operating system or browser, which, in turn, opens you up for an attack. What's most concerning about these attacks is users don't have to click, download or open anything to become infected. The best way to avoid these types of attacks is to keep your web browsers updated and ensure users don't navigate to potentially dangerous sites.
3. **Phishing attacks**—Phishing scams are a common strategy for hackers—one that requires minimal technical know-how and can be deployed via email. With every opened email, users risk becoming the victim of monetary loss, credit card fraud and identity theft. Successful phishing attacks oftentimes go unnoticed, which increases the risk of large and continued losses, particularly for businesses. To avoid becoming the victim of an attack, organizations need to train users on how to identify and avoid common phishing scams.

For more information on network security threats and prevention strategies, contact Hierl Insurance Inc. today.

Hierl Insurance Inc.
920-921-5921
www.hierl.com