ISSUE 06

Cyber Guardian

Publication for your online safety

2024

SRI LANKA CERT|CC
Sri Lanka Computer Emergency Rediness Team
Coordination Centre

An IBM report states that customers are also bearing the costs of data breaches.

According to IBM's 2024 Data Breach Report, released in July, the average cost of a data breach has risen to $4.88 million—a 10% increase compared to the previous year. The study, conducted by the Ponemon Institute and analyzed by IBM, offers an in-depth look at data breaches across 604 organizations worldwide. Insights were gathered from over 3,500 security and business professionals who experienced these incidents.

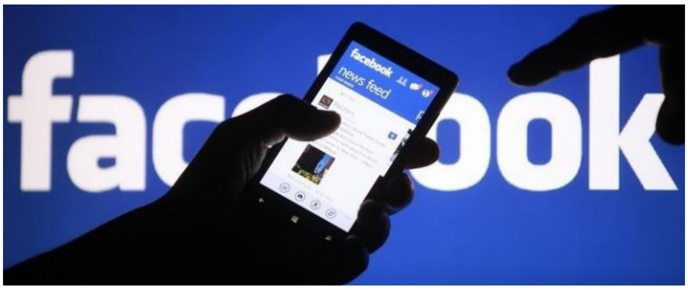
A key finding of the report is that consumers are shouldering part of the financial burden, as businesses transfer the costs of data breaches to their goods and services. This year, 63% of businesses reported that they would need to raise prices to offset losses caused by data breaches, up from 57% last year. These price increases stem from higher production costs, system downtime, and customer churn as clients switch to competitors.

Nearly 46% of the breaches involved customers' personal information, including Social Security numbers, emails, phone numbers, and home addresses. Additionally, 43% of the breaches involved sensitive corporate data, such as intellectual property and trade secrets.

One of the primary reasons for these breaches is a shortage of skilled cybersecurity personnel. More than half of the companies surveyed indicated they are struggling with severe staffing shortages in their security teams. While many are adopting new AI technologies to manage security, these teams are already under significant pressure.

@ The National Cybersecurity Alliance

What to do if Facebook is hacked?



If your Facebook account is hacked, it's important to act quickly to secure your account and protect your personal information. Here's what you should do:

1. Check if You Can Still Access Your Account

Log In: Try logging in with your usual credentials. If successful, immediately proceed to change your password and review your account settings.

Password Reset:If you can't log in, use the "Forgot Password" option on the Facebook login page to reset your password via your email or phone number.

2. Change Your Password

New Password: If you can access your account, change your password to something strong and unique. Avoid using common passwords or any that you've used on other platforms.

Enable Two-Factor Authentication: Set up two-factor authentication (2FA) to add an extra layer of security. This will require a code sent to your phone or email each time you log in from a new device.

3. Check and Secure Your Email Account

Email Access: Ensure that your email account associated with Facebook is secure. If hackers gain access to your email, they can control your Facebook account.

Change Email Password: If needed, change your email password and enable two-factor authentication there as well.

4. Report the Hack to Facebook

Report via Facebook's Help Center: Go to Facebook's Help Center and search for "hacked account." Follow the instructions to report that your account has been compromised.

Facebook Support: If you can't access your account at all, use Facebook's support options for hacked accounts. They might ask you to verify your identity by submitting an ID.

5. Review Account Activity

Check Recent Activity: Look at recent login locations and devices. If you see any suspicious activity, log out of all other sessions (you can do this via the Security and Login settings).Review Linked Apps: Check for any unknown apps or services linked to your Facebook account and remove them.

6. Notify Your Contacts

Warn Friends and Family: Let your contacts know that your account was hacked. This prevents them from falling victim to any messages or posts made by the hacker.

7. Monitor for Suspicious Activity

Watch for Phishing Attempts: Be cautious of emails or messages asking for personal information, even if they appear to come from Facebook.
Regularly Review Account: Continue to monitor your account for any unusual activity.

8. Consider Additional Security Measures

Identity Theft Protection: If sensitive information was exposed, consider using identity theft protection services.

Update Security Settings Regularly:Periodically review and update your security settings to keep your account secure.

9.Prevent Future Hacks

Use Strong, Unique Passwords: Avoid using the same password across multiple platforms.

Be Wary of Suspicious Links: Don't click on links in emails or messages unless you're sure they're legitimate.

Taking these steps should help you regain control of your Facebook account and protect it from future hacking attempts.

Cybercriminals like to go phishing, but you don't have to take the bait.

Phishing is when criminals use fake emails, social media posts or direct messages with the goal of luring you to click on a bad link or download a malicious attachment. If you click on a phishing link or file, you can hand over your personal information to the cybercriminals.

A phishing scheme can also install malware onto your device. No need to fear your inbox, though. Fortunately, it's easy to avoid a scam email, but only once you know what to look for. With some knowledge, you can outsmart the phishers every day.

See it so you don't click it.

The signs can be subtle, but once you recognize a phishing attempt you can avoid falling for it. Before clicking any links or downloading attachments, take a few seconds (like literally 4 seconds) and ensure the email looks legit. Here are some quick tips on how to clearly spot a phishing email:

Does it contain an offer that's too good to be true?

Does it include language that's urgent, alarming, or threatening?

Is it poorly crafted writing riddled with misspellings and bad grammar?

Is the greeting ambiguous or very generic?
Does it include requests to send personal information?

Does it stress an urgency to click on an unfamiliar hyperlinks or attachment?

Is it a strange or abrupt business request?

Does the sender's e-mail address match the company it's coming from? Look for little misspellings like pavpal.com or anazon.com.

Uh oh! I see a phishing email. What do I do?

Don't worry, you've already done the hard part, which is recognizing that an email is fake and part of a criminal's phishing expedition.

If you're at the office and the email came to your work email address, report it to your IT manager or security officer as quickly as possible.

If the email came to your personal email address, don't do what it says. Do not click on any links – even the unsubscribe link – or reply back to the email. Just use that delete button. Remember, DON'T CLICK ON LINKS, JUST DELETE.

You can take your protection a step further and block the sending address from your email program. (Outlook. Gmail. Mac Mail. Yahoo! Mail)

Picture Story

Capacity Building Program on Cyber Security Systems in Gampaha

A capacity development program on cybersecurity systems for government institutions was recently held at the Gampaha District Secretariat Auditorium, chaired by Mr. Lalinda Gamage, Gampaha District Secretary/District Governor.

The program was conducted in collaboration with the Sri Lanka Computer Emergency Response Team (Sri Lanka CERT) and the Ministry of Home Affairs. It was attended by officials related to information technology, including divisional secretaries from the Gampaha District.