ISSUE 05

2024

Cyber Guardian

Publication for your online safety

Steps Taken to Establish the National Cyber Security Operations Center in Sri Lanka

Sri Lanka CERT is the National Center for Cyber Security and holds the national responsibility to protect the country's cyberspace from cyber threats. Sri Lanka CERT is taking steps to establish the National Cyber Security Operations Center to ensure the cyber security of public sector institutions providing critical services. In the coming years, Sri Lanka CERT aims to connect 40 identified critical service providers to the NCSOC.

By introducing the necessary technologies, it will be possible to detect cyber events in real-time and response to those events in real time manner. A reputed company, Sentry Labs, in collaboration with VSIS, is providing software solutions for the NCSOC. The agreement signing took place recently at the Sri Lanka CERT.

How Phishing Scams Work as Friend Requests

Phishing scams can indeed appear in the form of a friend request on social media platforms. Here's how this works:

1. Fake Profiles

Scammers create fake social media profiles that look convincing, often using stolen photos, names, and other details to appear legitimate. These profiles might mimic real people or organizations, or they may simply seem like friendly strangers.

2. Sending the Friend Request

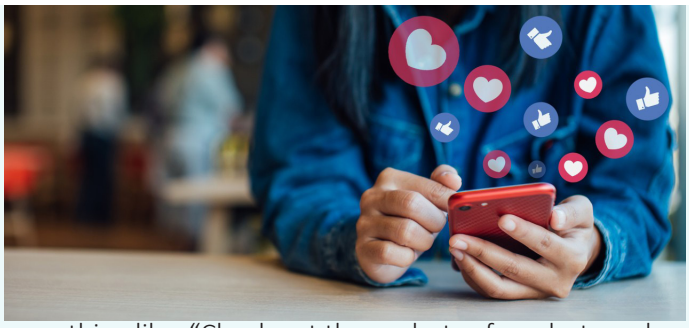
Once the fake profile is set up, the scammer sends friend requests to a wide range of users. The goal is to get you to accept the request, giving the scammer access to your personal information and potentially your friends list.

3. Gaining Trust

After the friend request is accepted, the scammer might start interacting with you to build trust. This could involve casual conversations, liking your posts, or commenting on your photos to make the connection seem more genuine.

4. Initiating the Phishing Attempt

Once trust is established, the scammer might send you a direct message with a malicious link, claiming it's something interesting or urgent. The message could be



something like, "Check out these photos from last weekend!" or "You've won a prize, click here to claim it!"

The link might lead to a fake login page for a popular service, such as Facebook, where you're asked to enter your username and password. If you do so, the scammer captures this information.

5.Further Exploitation

With your login details, the scammer can access your account, steal more information, and potentially use your account to send phishing messages to your friends, spreading the scam further.

Protecting Yourself from Phishing Scams in Friend Requests:

1. Be Cautious of Unknown Requests

If you receive a friend request from someone you don't know, especially if the profile looks new or has very few posts, be cautious. Scammers often create fake profiles that lack real content.

2 Verify the Profile

If the request seems to come from someone you know, double-check their profile to ensure it's legitimate. Look for mutual friends, real interactions, and consistent activity. You can also reach out to the person via another method to confirm it's really them.

3. Avoid Clicking Suspicious Links

Even if the request is from someone you know, be wary of any unexpected messages that contain links, especially if the message seems generic or out of character for that person.

4.Report Suspicious Activity

If you suspect a friend request is part of a phishing scam, report the profile to the social media platform. This helps prevent the scammer from targeting others.

We often think of cybersecurity in terms of our physical health

SCAM

Cyber resilience is another way to think about your online fitness: just like humans can get sick even if they take precautions like washing their hands, taking vitamins, or exercising, your online systems can be attacked even if you follow cybersecurity best practices. Cyber resilience is how you get better. It might take a bandage or extensive surgery, but you can recover. That's why you should have a plan.

Today, cyber resilience is a critical concept that emphasizes the ability to withstand and recover from cyberattacks, as well as the capability to adapt to new threats. Individuals, businesses, and other organizations can assess their own resilience and bolster their cyber resilience strategies.

Understanding cybersecurity resilience

Generally, cybersecurity resilience is the backbone of an organization's ability to maintain essential functions and swiftly recover from cyber incidents. It encompasses proactive measures, incident response readiness, and recovery strategies.

Resilience goes a step beyond basic cybersecurity measures because cyber resilience emphasizes the ability to operate during a cyber incident as well as recovery. Simply put, it's about staying operational and safeguarding critical data despite cyber threats. It's a way to think "when" instead of "if."

Effective resilience helps minimize the impact of attacks, reduces downtime, protects sensitive data, maintains customer trust, and complies with regulatory requirements. It safeguards an organization's reputation and financial stability.

Assess your personal cyber resilience

While we typically speak of cyber resilience as a strategy for organizations, evaluating your cyber resilience as an individual is a good thought exercise. This can be a first step before embarking on a plan to strengthen your business, nonprofit, school, or group. Consider your own digital habits, security practices, and awareness of potential threats.
Ask yourself:

Do I use long, complex, and unique passwords?

Do I have MFA enabled for every account?

Do I regularly update software?

Do I refuse to click suspicious links or download unknown attachments?

Do I back up important data and know how to recover it in case of a cyber incident?

@The National Cybersecurity Alliance.

Pictuer Story

A Southern Province Cyber Security Workshop

A one-day cyber security awareness workshop for Southern Province government officials and IT officials was held at Galle Southern Province Management and Development Center recently.
A group of nearly 150 officials attended this workshop organized jointly by the Sri Lanka Cert and the Southern Province Chief Secretariat