ISSUE 04

Cyber Guardian

2024

Publication for your online safety

Sri Lanka Computer Emergency Readiness Team Coordination Centre

Sri Lanka CERT Issues Warning About Social Media Scams

Sri Lanka CERT urges the public to be cautious of fake messages purportedly sent by various banks, commercial institutions, and international organizations. These scams promise donations, cash gifts, lucky draws, and job insurance, using the names of legitimate entities.

Cyber criminals attempt to contact individuals through fake websites, social media platforms, SMS, and WhatsApp. By accessing the links provided in these messages, they can steal data from computers and mobile phones, leading to various forms of abuse and financial fraud.

The Sri Lanka CERT reports that these types of crimes have been increasing recently, with a growing number of victims. Fraudsters often operate around national and religious festivals, exploiting the public's trust during these times. In response,

Sri Lanka CERT and other organizations have launched extensive awareness campaigns. Despite these efforts, the number of complaints from victims continues to rise due to ignorance and neglect.

Sri Lanka CERT advises the public to verify any suspicious messages by visiting the official websites of the respective institutions, contacting them through official phone numbers, or making inquiries before responding to such messages on the internet and social media.

Sri Lanka CERT further requests the public to refrain from opening or responding to unverifiable messages, emphasizing the importance of staying vigilant against these scams.

Play safe while gaming!

Whether your eSports pro, killing a few spare minutes on your phone, or enjoying an endless fantasy realm for hours, who doesn't love online gaming? Remember, though, that you shouldn't lower your cybersecurity defenses just because you're racking up points. Here are our 10 top tips for staying safe online with a joystick, or angry bird, in your hand!

1. STRONG PASSWORDS FOR THE WIN!

Winners use long, complex, and unique passwords.
The strongest passwords are at least 12 characters long and include letters, numbers and symbols. Ideally, your password is not recognizable as a word or phrase. And, yes, you should have a unique password for each online account. Sounds hard to remember? Using a password manager has never been easier – many smartphones and web browsers include password managers. The best password managers will even suggest strong passwords.

2. RESEARCH YOUR GAMES

Mobile gaming makes up almost half of the global games market! Just because a game is available on a trusted app store, doesn't guarantee it is a safe app to download. Before downloading any new gaming app on your device, make sure it's legitimate. Check out the reviews and look it up on a search engine before downloading.

3. FLIP ON MFA

Multi-factor authentication (MFA), sometimes called 2-factor authentication, adds a whole other level of security to your accounts, and now some games and gaming systems allow for MFA. MFA includes biometrics (think face ID scans or finger-print access), security keys, or apps that send you unique, one-time codes when you want to log on to an account. We recommend you use MFA whenever offered. It's like building a castle around your loot crate!

4. MAKE UPDATES AUTOMATIC

We recommend keeping your gaming hardware and software as updated as possible. You don't have to check your Settings tab every morning – you can usually set up automatic updates so that updates are downloaded and installed as soon as they are available from the device, software, or app creator. Note that you might have to restart your device for the updates to fully install. It is best to do this right away, but you can often schedule this to happen during times when you aren't gaming, like the middle of the night (or perhaps the early afternoon).

5. DON'T TAKE THE BAIT

Cybercriminals often entice gamers into clicking bad links or downloading malicious files by offering cheats or hacks – this is known as phishing. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting. If the offer seems too good to be true, chances are it is. Verify the link before clicking it by hovering over it with your cursor to see the link's true destination.

6. CREDIT, NOT DEBIT

If a gaming system requires you to tie a specific payment method to your account, choose a credit card over a debit card. Credit cards come with more consumer protection than debit cards, and you have a better chance of getting your money back in case of fraud.

7. SHARE WITH CARE

The more information you post, the easier it may be for a criminal to use that information to steal your identity, access your data, or commit other crimes, such as stalking. Think about how much personal information you provide on gaming account profiles. Err on the side of sharing less online. And if a stranger asks you to share this information, say no.

8. GAME IN DISGUISE

Are you suiting up and playing with people you don't know? They don't need to know your real name or any other personal information — they just need to find out how awesome you are at the game. Use a safe game name: something cool like National Cybersecurity Awesome or Disguised Gamer99. Don't use your first or last name in your usernames. Use an avatar instead your actual photo. If a stranger asks you to share a photo or to turn on your webcam, refuse. They don't need to see you to play you.

9. NO SHAME IN A STRONG BLOCKING GAME

If another player is making you feel uncomfortable, block them! Tell a trusted adult. Remember that you can always kick a player out of the game if they are being a bully or otherwise making you uncomfortable. We have a database with info on blocking people on a bunch of platforms. Hurtful comments online can have a real impact on your mental health — if you feel like hurting yourself, you should reach out to someone you trust immediately.

10. CHECK YOUR SETTINGS

As soon as you get a new gaming console or try out a new game, open its privacy and security settings. Configure them to your comfort level. Remember, many game makers default to the least secure settings, and you shouldn't assume those default settings are set to what you would like. Your game might default to sharing your behavior and location data with the manufacturer, for example. Think about what sort of data you're comfortable with sharing.

Our Services

SECURE NETWORK AND CLOUD INFRASTRUCTURE

We are dedicated to fortifying your network and cloud infrastructure to ensure the utmost security of your digital assets. We offer comprehensive security assessments to identify vulnerabilities and design tailored solutions to address them effectively. Our expertise lies in implementing robust authentication and access control mechanisms, encrypted data transmission, and real-time threat detection systems. With a focus on best practices, we configure and monitor firewalls, routers, and cloud security services to prevent unauthorized access and data breaches. By partnering with us, you can trust that your network and cloud infrastructure are fortified against potential cyber threats, enabling you to conduct your business with confidence and peace of mind.

- **Internal and External Network Vulnerability Assessments.**
- **Penetration testing,**
- **Cloud security reviews.Wireless network security reviews.**
- **Network architecture reviews**
- **Firewall rule-based reviews.**
- **Configuration reviews of routers and switches.**
- **Server OS configuration reviews.**
- **Data center physical security reviews.**

Pictuer Story

National Cyber Security Operations Center (NCSOC).

V S Information Systems (Pvt) Ltd and Dialog Broadband Networks in joint collaboration with Sri Lanka CERT, for the establishment of the National Cyber Security Operations Center (NCSOC).