ISSUE NO 04

NOVEMBER 2023

Cyber Guardian

A Publication on Online Safety

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

SECURITY

Tips For Secure Online Shopping

Cybercriminals often target online shoppers to steal their money or personal details. They employ various methods, including setting up fake retailer websites, selling nonexistent products, requesting unnecessary personal and payment information, and installing malicious software ("malware") on your device. It is crucial to stay vigilant and ensure security when shopping online.

Once cybercriminals obtain your financial details and money, it is unlikely that you will recover your funds. Not only will you be disappointed that your goods never arrived, but you will also have lost the money you paid for them. When using personal devices (e.g., smartphones, tablets, computers, and laptops) for online shopping, there are several factors to consider. Follow our security tips to guarantee a secure online shopping experience.

Shop Using Secure Devices:
Ensure that the devices you use for online shopping have the latest updates installed and are connected to a trusted network. For example, use your home Wi-Fi or (4G/5G) cellular network instead of public Wi-Fi.

Protect Your Payment Information and Accounts:
Be cautious about saving payment information on an online shopping account. If you do, enable multi-factor authentication (MFA) to enhance protection. If MFA is not available, set a long, complex, and unique passphrase as the account's password. Consider using a password manager to generate and store passwords for you.

Use Trusted Sellers:
Research online shopping websites before making a purchase and stick to well-known, trusted businesses.

Know the Warning Signs:
Extremely low prices, payments through direct bank deposits, and online stores with limited information on delivery, return, and privacy policies can be signs of a scam.

Use Secure Payment Methods:
Never pay by direct bank deposits, money transfers, or digital currencies such as Bitcoin, as it is rare to recover money sent this way. Opt for secure payment methods

like PayPal or credit cards. Consider setting up a dedicated card with a low credit limit specifically for online shopping to minimize financial losses if your card details are compromised.

Don't Engage and Report Suspicious Contact:
Be cautious of strange phone calls, messages, or emails about online orders. If someone contacts you about an order you don't remember placing, it could be a scam. Stop contact and reach out to the store using the details on their official website to verify.

Watch Out for Fake Delivery Scams:
Stay vigilant while waiting for your goods to arrive. Cybercriminals can send fake parcel delivery notifications with links that may trick you into downloading malware or providing personal details. If you receive such a message, do not click on the link; delete the message immediately.

Services

DIGITAL FORENSICS

Sri Lanka CERT specializes in digital forensics and providing cutting-edge investigative services to uncover and analyze digital evidence.

We assist individuals and organizations in resolving complex cyber incidents, data breaches, and unauthorized access. Our forensic experts employ state-of-the-art tools and methodologies to acquire, preserve, and analyze digital data from various sources.

Whether identifying the source of a cyber attack, recovering deleted files, or presenting expert testimony in legal proceedings, we offer reliable and efficient solutions. With our digital forensics services, you can gain crucial insights into digital incidents, take appropriate actions, and enhance your overall cybersecurity posture.

Our services include:

- Investigations on counterfeit payment devices (in accordance with the Payment Device Fraud Act)
- Malware incidents
- Email-related digital forensic investigations.
- CCTV video footage enhancements
- Data recovery
- Data wiping

Hot Line -101 report@cert.gov.lk www.cert.gov.lk www.onlinesafety.lk

Protect Yourself from Scams

Being alert to scam messages is a great way to protect yourself online. Learn to spot scams. Don't click on links if you suspect the message might not be legitimate. Often, scammers pretend to be a person or organization you trust.

Avoid downloading files if they have a different file extension than what you were expecting (for example, a file that ends in .exe or .msi when you were expecting a PDF or image).

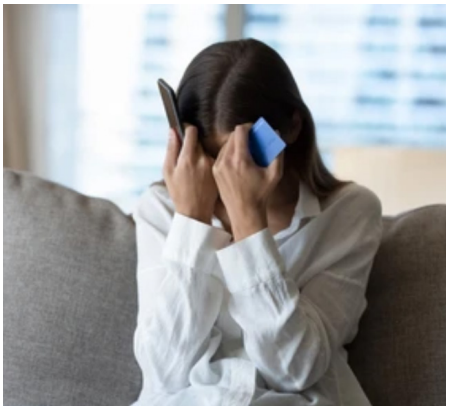
Disable image previews in your emails from non-trusted sources. Viruses can attach themselves to images; this feature can be disabled in the settings or options of the program you are using.

Don't download applications from third-party download sites that are not widely known to be legitimate. Use the official store for your device instead, such as the Apple App Store, the Google Play Store, or the Microsoft Store.

Avoid clicking on online ads to download applications, and use ad-blocking software.

Don't download and install applications from peer-to-peer networks; you never know who may have altered the files.

Exercise caution with links in emails or instant messages, and avoid executing attachments unless you are certain they are legitimate. Use a spam filter to protect yourself from malicious messages. If you need to log in to a service or account, visit their website directly rather than clicking on a potentially illegitimate link.



What is personal data?

A data contributor, such as a name, an identification number, gender data, or an online address, or one or more factors specific to the physiological, physical, genetic, psycho-economic, cultural, or social identity of that person or natural person, directly or otherwise. Any information that can identify an individual is encompassed in this concept.

This can be more simply expressed in colloquial terms as 'data' defined as any information that can identify an individual, including name, identification number, location data, physical, physiological, genetic, psychological, economic, cultural, or specific factors for social identification. Data protection is the right to ensure that an individual's personal data is not used, exchanged, or maintained without their knowledge.

VPN

VPN connections use cryptography to protect sensitive information in untrusted networks. To safeguard this traffic and ensure data confidentiality, VPNs encrypt your information not only from hackers but also from your internet service provider.

These measures make it more difficult for others to monitor and gather information about your online activities, enhancing your protection when using public networks.

While using a good VPN is strongly recommended, it's essential to install updates regularly to ensure you receive all security patches. Additionally, continue to use two-factor authentication for added security