الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Cybersecurity Guidelines for E-commerce Consumers

(CGEC – 1: 2019)

Sharing Indicator: White
Document Classification: Open

In the Name of Allah,
the Most Gracious,
the Most Merciful

Disclaimer: The following controls will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interpretation of this document.

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

Red - Personal, Confidential and for Intended Recipient only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients either inside or outside the organization.

Amber - Restricted Sharing

The recipient may share information classified in amber only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

Green - Sharing within the Same Community

The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organization. However, it is not allowed to exchange or publish this information on public channels.

White - No Restrictions

Table of Contents

Executive Summary

E-commerce is considered one of the national transformation program's goals, that support the achievement of the kingdom's vision 2030. Saudi Arabia is one of the largest e-commerce markets in the Middle East and North African region. Given the rapid growth of e-commerce in the Kingdom, and considering the increased threat landscape on consumers, the E-commerce Law was approved by the Council of Ministers, which aims at enhancing the reliability of e-commerce in the Kingdom, in addition to increasing e-commerce's contribution to the national economy, and motivating and improving e-commerce activities in the Kingdom.

The National Cybersecurity Authority (NCA) developed the Cybersecurity Guidelines for E-Commerce Consumers (CGEC - 1: 2019) to assist consumers within the Kingdom around best practices to secure their devices, systems, online accounts, data and payments during their online e-commerce channels.

The main guidelines categories within the CGEC are:

1. Protect Your E-commerce Accounts and Devices
2. Secure Your E-commerce Transactions
3. Exercise Caution When Communicating Online for E-commerce
4. Limit Sharing Your Personal Information

Detailed guidelines are highlighted within this document for each one of the categories above.

Introduction

The National Cybersecurity Authority (referred to in this document as "NCA") developed the Cybersecurity Guidelines for E-commerce Consumers (CGEC - 1: 2019) after conducting a comprehensive study of multiple national and international cybersecurity e-commerce guidelines, studying related national initiatives, statistics and regulatory requirements; reviewing and leveraging cybersecurity best practices and analysing previous cybersecurity incidents and attacks on consumers.

According to a recent study[1] of the market in Saudi Arabia, around 58% of the population in the Kingdom has shopped online at least once every three months, spending an average of SAR 4,000 on online shopping annually. Given the increased use of mobile solutions , such as mobile apps, and the growing convenience of online shopping, these numbers are likely to be higher. According to the same study, a significant number of the Saudi population have made purchases from companies based in other GCC countries and outside the region, while only a fraction of consumers (7%) have purchased exclusively from Saudi-based e-commerce service providers.

The main drivers of the rapid growth and adoption of e-commerce are the convenience of home deliveries, the timesaving benefits of e-commerce, the attractive Internet offers, and the wide range of products from which to choose. However, this has created new types of threats which these guidelines are trying to address.

Scope of Applicability

These guidelines target all consumers in Saudi Arabia who are conducting e-commerce through any channel (e.g., social media, websites, apps) using any computing device (e.g., personal computers, tablets, smart phones and TVs).

These guidelines are for awareness purposes and are intended to help consumers navigate a secure e-commerce experience.

[1] E-Commerce in Saudi Arabia, Communications and Information Technology Commission, 2017

Cybersecurity Guidelines for E-commerce Consumers

1. Protect Your E-commerce Accounts and Devices

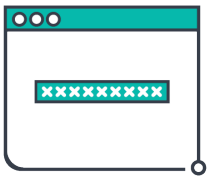
1-1 USE ANTI-VIRUS SOFTWARE

- Use anti-virus software on all your devices, especially the ones you often use for e-commerce. If your device does not have a pre-installed anti-virus software, it is recommended that you install one before conducting any e-commerce transaction.
- Make sure you use trusted and official versions of anti-virus software products.

1-2 USE DIFFERENT PASSWORDS

- If you are shopping on multiple apps or websites, use a different password for each. Similarly, use different passwords for your devices and social media accounts.
- Also, to protect your digital identity, make sure to change your passwords periodically and never share your passwords with others.

1-3 CREATE STRONG PASSWORDS



- When creating a password for your e-commerce account, follow these best practices:
  - Avoid using common everyday words (e.g., “password”, “qwerty”), personal information (e.g., date of birth, graduation year) or sequential numbers (e.g., “123456”).
  - Do not write it down.
  - Make it as long and complicated as possible, using combination of special characters (such as @#$%^&), upper case and lower-case letters and random numbers.

1-4 CONSIDER USING ADDITIONAL VERIFICATION OPTIONS

- If available, consider using additional verification mechanisms (such as email messages) offered by e-commerce apps or websites (including social media accounts).
- Choose to shop online with e-commerce service providers who provide that extra verification protection option.

1-5 UPDATE APPLICATIONS REGULARLY

- Keep all your applications (including operating system and anti-virus software) on your devices up to date. This can be done either automatically (by enabling that feature on your device) or manually (by dedicating a fixed time of the week/month to run the update).

1-6 BACK UP YOUR DATA

- Back up your data by, for example, copying it to your computer or to an external hard drive to avoid losing your data in case of your device (which you use for e-commerce) got infected with viruses.
- Enable the automatic back up feature, if available on your device.

1-7 CHANGE DEFAULT SETTINGS ON YOUR DEVICES AND ACCOUNTS

- Review and change the default security and privacy settings on your accounts and web browser to, for example, avoid saving social media login credentials, payment or bank account data.

1-8 PAY ATTENTION TO SECURITY WARNINGS

- Do not ignore security warnings (e.g., alerts of unverified e-commerce service providers or non-secure websites) that may come up on your screen.
- Make sure that you read and understand them before taking any further actions.

2. Secure Your E-commerce Transactions

2-1 REVIEW YOUR TRANSACTIONS PERIODICALLY

- Review your bank (specifically your credit card) statements and electronic wallets (eWallets) transactions periodically. Call your bank right away if you see any suspicious fraudulent purchases. Stop your credit card immediately, through, for example, your bank's app or website, when your card is stolen. The sooner an online fraud is detected, the faster other consumers can also be alerted by the bank.
- Make sure your contact information with your bank is up to date.
- Enable SMS notifications on your credit card/eWallet to stay informed about any transactions on your account.

2-2 USE A DEDICATED CREDIT CARD

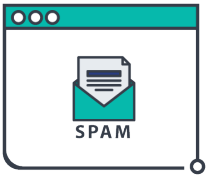
- If you own multiple credit cards, try to use a dedicated one for e-commerce purchases.
- If offered by your bank, use a low limit card or a pre-paid one.

2-3 SECURE YOUR ELECTRONIC WALLET

- Make sure to protect access to your eWallet with a strong authentication mechanism (e.g., password). eWallets are becoming more popular and widely used by consumers, therefore attacks related to these payment methods are rising.
- Frequently check your eWallet account for suspicious activities (e.g., failed login attempts).

3. Exercise Caution When Communicating Online for E-commerce

3-1 PROTECT YOUR ACCOUNT AGAINST UNWANTED MESSAGES (SPAM)

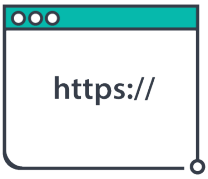


- Activate the spam filter on your email. Many email services (especially web email) have a filter included.
- Report spam messages (email/social media) immediately to your email provider/social media platform.
- Dedicate an email account to be used for e-commerce.

3-2 BE AWARE OF FRAUDULENT CALLS

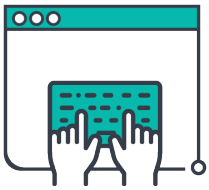
- Be aware of fraudulent calls. A common scam is fraudulent calls from fake e-commerce service providers who normally have fake websites/ social media profiles.
- Make it a strong preference to shop and interact only with verified e-commerce service providers. Online review platforms (such as Ma'aroof [2]) are a good way to check an e-commerce seller's authenticity and reputation.

3-3 USE SECURE WEBSITES



- Before you enter your personal or financial details, make sure that the website's URL starts with (https://) instead of (http://).
- Avoid e-commerce service providers who do not offer this enhanced security, as this security feature means the website is using trusted encryption protocols to protect your personal and financial information.

[2] https://maroof.sa



3-4 BE AWARE OF SUSPICIOUS URLS

- Avoid clicking on links you see on messages (email, SMS, or social media) or web (usually in advertisements), as these may redirect you to fake websites.
- Be aware of fake websites which, for example, offer unrealistic prices for products.

3-5 SHOP USING SECURE APPS, DEVICES AND NETWORKS

- Be aware of fake apps and websites. Those can be avoided by, for example, downloading apps from the official app stores.
- It is highly recommended to avoid conducting e-commerce transactions or entering your social media credentials on public devices (e.g., business center computers at hotels) or connecting to public Wi-Fi networks (e.g., airport Wi-Fi).

3-6 REPORT INCIDENTS QUICKLY

- If your e-commerce account has been hacked, act fast and inform the merchant.
- If your payment card information has been stolen, contact your bank immediately.
- If your device has been compromised, contact local authorities. The earlier you report any incident, the more you can limit damages.

4. Limit Sharing Your Personal Information

4-1 READ THE PRIVACY POLICY

- Shop only with reputable e-commerce service providers who have a privacy policy posted. Read the policy and make sure it clearly explains how your data will be used and stored by the seller.
- Avoid e-commerce service providers whose policy includes misuse of personal data (e.g. giving consumers' personal information (without their consent) to advertisement agencies).

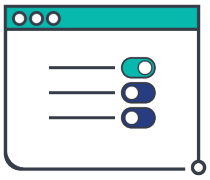
4-2 PROTECT YOUR PERSONAL INFORMATION

- Do not give more personal information than needed when signing up for an e-commerce account or shopping online.
- Only share the information that is required to enable the specific e-commerce transaction and do not choose to save or store your personal or financial information on the apps or website.
- Avoid sharing your credit card details over non-secure communication channels such as email or social media messages.

4-3 IGNORE PHISHING MESSAGES

- Avoid phishing messages by checking the sender's identity carefully before opening the message. Phishing is a message that appears to be from a legitimate sender and intends to trick the recipient to reveal personal information such as username, password or credit card details.

4-4 LIMIT PERMISSIONS GRANTED TO APPS



- Carefully consider whether it makes sense to give mobile apps or websites permissions to access a variety of data and functions on your device (e.g., location, camera, address book or microphone).

Appendix A: Terms and Definitions

The table below highlights some of the terminologies contained herein, and the meanings ascribed thereto.

Term	Definition
Attack	Any kind of malicious activity that attempts to achieve unauthorized access, collection, disabling, prevention, destruction or sabotage of the information system resources or the information itself.
Backup	Files, devices, data and procedures available for use in case of failure or loss, or in case of deletion or suspension of their original copies.
Cybersecurity	According to the Royal Decree number 6801, dated 11/2/1439H, cybersecurity is the protection of networks, IT systems, operational technologies systems and their components of hardware and software, their services and the data they contain, from any penetration, disruption, modification, access, use or unauthorized exploitation. The concept of cybersecurity also includes information security and digital security.
E-commerce Service Provider	Merchant (person who is bound by commercial registration and using e-commerce) or practitioner (person who is not bound by commercial registration but using e-commerce).
Hyper Text Transfer Protocol Secure (HTTPS)	A protocol that uses encryption to secure web pages and data when they are transmitted over the network. It is a secure version of the Hypertext Text Transfer Protocol (HTTP).
Incident	A compromise through violation of cybersecurity policies, acceptable use policies, practices incident or cybersecurity controls or requirements.
Phishing	The attempt to obtain sensitive information such as usernames, passwords, or credit card details, often for malicious reasons and intentions, by disguising as a trustworthy organization in email, text or social media messages.

Privacy	Freedom from unauthorized interference or disclosure of personal information about an individual.
Threat	Any circumstance or event with the potential to adversely impact organizational operations or person (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority