الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Cybersecurity Guidelines for E-commerce Service Providers

(CGESP – 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's e-commerce spending is estimated to be SAR 26.8 billion in 2019[1], making the country one of the largest e-commerce markets in the Middle East and North Africa (MENA) region. Given the rapid growth of e-commerce in the Kingdom, and considering the increased threat landscape on e-commerce, 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 Service Providers (CGESP – 1: 2019) to educate and assist Small and Medium Enterprises (SMEs) and Small Office / Home Office (SoHo) e-commerce service providers within the Kingdom on implementing best practices to secure their business, devices, data, customer accounts and payments processes while providing a smooth online shopping experience for consumers.

The main guidelines categories within the CGESP are:

1. Use Strong Authentication
2. Protect Your E-commerce Systems
3. Minimize Impact of Data Breaches
4. Guard Your Social Media Accounts Used in E-commerce
5. Defend Your Network
6. Continuously Educate and Train Your Employees
7. Strengthen Your Internal E-commerce Infrastructure

[1] Statista eCommerce Report, 2019

Introduction

The National Cybersecurity Authority (referred to in this document as "NCA") developed the Cybersecurity Guidelines for E-commerce Service Providers (CGESP – 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 e-commerce service providers.

In the Kingdom, 26% of Small and Medium Enterprises (SMEs) use social media[2] to promote their products. Around 86% of the SMEs selling online say they have been active as online sellers for the last three to five years. Most of these e-commerce service providers focus on the Saudi Arabian market, while a few also target the wider GCC and Middle East markets. On the other hand, almost all Small Office / Home Office (SoHo) e-commerce service providers (sometimes also referred to as Online Seller, C2C, Consumer-to-Consumer, Micro Enterprises, or Sole Proprietorships) generate sales by leveraging social media platforms to reach customers and boost traffic.

The massive increase in the uptake of e-commerce has led to a new generation of associated cybersecurity threats. Some threats are accidental while others are done deliberately by hackers or criminals (collectively referred to as attackers in this document). Common security threats include e-commerce system and data compromise, denial of service and click fraud. Such threats can lead to decrease in revenue, loss of inventory, IT systems or website being unavailable, this leads to negative reputation and other legal consequences.

These guidelines are designed to help SME and SoHo e-commerce service providers in the Kingdom to better understand the e-commerce cybersecurity risks they face and provide them with practical advice on how to better protect their businesses, systems and data from cyber threats.

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

Scope of Applicability

These guidelines are applicable to e-commerce service providers in Saudi Arabia who fall into the following two segments[3]:

- SME (Small and Medium Enterprises).
- SoHo (Small Office / Home Office).

The guidelines cover conducting e-commerce using any channel (e.g., social media, websites and apps) using any computing device (e.g., personal computers, tablets, smart phones and TVs).

These guidelines are for awareness purposes. However, the NCA strongly encourages every e-commerce service provider in the Kingdom to use these guidelines to implement best practices to minimize cybersecurity risks to their businesses, systems and data. Furthermore, due to the ever-changing nature of cyber threats, e-commerce service providers are encouraged to do their own research to see if additional cybersecurity measures are required.

[3] Small and Medium Enterprises General Authority (Monsha'at)

Relationship to Other National Cybersecurity Publications

In addition to the CGESP, the NCA has also developed the Cybersecurity Guidelines for E-commerce Consumers (CGEC – 1: 2019) which is intended for educating e-commerce consumers in the Kingdom. Large enterprises (another segment of e-commerce service providers) should refer to NCA's Essential Cybersecurity Controls (ECC – 1: 2018) for guidance and in some cases for mandatory compliance.

The CGESP complements other related national laws, regulations, frameworks and standards overseen by the following organizations:

- Ministry of Commerce and Investment (e.g., E-Commerce Act).
- National Cybersecurity Authority (e.g., Data Protection Act – under development).
- Saudi Arabian Monetary Authority "SAMA" (e.g., Cyber Security Framework, Banking Consumer Protection Principles and other related cybersecurity publications by SAMA).

Cybersecurity Guidelines for E-commerce Service Providers

The guidelines detailed in this document are organized around seven categories. Some guidelines apply to Small and Medium Enterprises (SMEs) e-commerce service providers, or Small Office / Home Office (SoHo) e-commerce service providers, or both as follows:

👥 Applies to SME e-commerce service providers

👥 👤 Applies to both SoHo and SME e-commerce service providers

	1. Use Strong Authentication	Scope of Applicability
1-1	**Avoid using predictable, shared or old passwords**	👤 👥
	In order to protect your e-commerce accounts as a service provider, use strong passwords that are: • Made up of random sequence of letters (both upper case and lower case), numbers, and special characters (!@#$%^&*). • Not common words, simple sequence of numbers (e.g., “123456”) or any personal information, such as your birthday or child’s name, as these are easy to guess. • Long (at least 8 characters long), which makes it harder for attackers to break it. Make sure to change passwords at least every 3 months and never disclose passwords to others.	
1-2	**Change all default passwords**	👤 👥
	Some systems and devices come with default admin passwords. Change these immediately upon installation and before use. Default passwords are known by attackers and can be used to attack and access your e-commerce systems. Use a different password for each one of your e-commerce systems, applications and accounts.	
1-3	**Consider using multi-factor authentication**	👤 👥
	For systems or applications that handle consumer login, consider deploying a multi-factor authentication feature to protect your consumers’ accounts. For example, when a consumer logs in with a password, they may be sent a code (via text message on their registered mobile phone) which they have to enter to complete the login process. Also, consider protecting your own e-commerce account by signing up for additional authentication mechanisms (such as email messages) offered by e-commerce apps or websites (including social media accounts).	

	2. Protect Your E-commerce Systems	Scope of Applicability
2-1	**Know your e-commerce technology assets**	👤 👥
	Keep an up to date list of all the current IT equipment, software, data and any other technology assets you use for e-commerce. The first step in protecting your e-commerce systems is knowing what devices and data are critical to your business. Usually, these are the assets that your e-commerce business cannot function without.	
2-2	**Control number of admin accounts**	👥
	Grant your e-commerce business employees the lowest level of user rights required to perform their job duties. An admin account is a high privilege user account that has more power to make changes in the system than other user accounts. Admin privileges may be given very carefully, and every access to the admin account should be strictly controlled through a more stringent password/multi-factor authentication and a shorter timeout period. You should also review users' access periodically and limit the number of users who have remote access to your systems.	
2-3	**Use anti-malware software**	👤 👥
	To protect your e-commerce systems from malware (e.g., viruses), use and regularly update anti-malware software on every device in your e-commerce business ecosystem (including computers, smart phones, and tablets). It is recommended to set the anti-malware software to automatically check for updates at least daily, and set to run a complete scan on a regular basis.	
2-4	**Regularly update your applications on all devices**	👤 👥
	Keep all your e-commerce devices and applications (especially operating systems) up to date with security patches and vendor upgrades.This is one of the most effective ways to protect against malware and viruses.	
2-5	**Stay up to date with cybersecurity threats**	👤 👥
	Subscribe to vendor notifications and cybersecurity alerts to keep up to date on cybersecurity trends and active threats. You may also follow latest updates from trusted organizations (e.g., Computer Emergency Response Team for cybersecurity – Saudi Arabia (CERT-SA)) to learn more about cybersecurity trends and publications.	

2-6	**Avoid connecting to non-secure wi-fi networks**	👤 👥
	Avoid using non-secure networks (e.g., public Wi-Fi) for any business transaction. These networks are an ideal location for attackers to intercept data transmission and obtain your data such as login details and financial information.	
2-7	**Use encryption on your website**	👤 👥
	Consider using an encryption protocol to secure your e-commerce website. Such protocols are a good way of ensuring that transactions conducted on your e-commerce website are secure. This is done by encrypting any data that gets inputted to your website.	
2-8	**Use trusted websites to display your ads**	👤 👥
	Protect against fraudulent clicks on your ads by running your ads on trusted websites which you know are more likely to have actual customers.	

	3. Minimize Impact of Data Breaches	Scope of Applicability
3-1	**Back up your data**	👤 👥
	Consider backing up your critical data, which may include your business, social media and customer information. You can use external online backup services (e.g., cloud backup) or external storage media (e.g., external hard drive). If you choose to use a cloud service for backup, refrain from storing your Saudi customers' data in the cloud if that provider operates outside the Kingdom, in order to comply with related and applicable national cybersecurity and data protection laws and regulations. Furthermore, perform backups regularly, at least on a weekly basis and check backup tools effectiveness by validating data on these backups to avoid data loss.	
3-2	**Protect your data with encryption**	👤 👥
	Encrypt all the critical data stored on your computer, cloud or external drive, and data sent over email. Encrypt sensitive files on portable storage (e.g., USB flash drive) so that data cannot be accessed by others in case you lost the portable storage.	
3-3	**Protect customers' financial data**	👤 👥
	Follow data minimization principles to reduce the amount and type of consumers' data you collect and keep. If you choose to store your customer's payment data (e.g., credit card details) on your e-commerce platform, make sure to apply strict cybersecurity controls (e.g., limited access, encryption) on such data to protect your business against a payment data breach. Also make sure to comply with any relevant national or international cybersecurity laws and regulations. For example, if you have customers outside Saudi Arabia, make sure to learn about any relevant mandatory requirements that your business must comply with (e.g., GDPR for EU customers). Make sure you report to SAMA and your customers any data breaches affecting your customers' payment data.	

3-4	**Change your default security settings**	👤 👥
	Review and change the default preferences in your web browser and e-commerce apps to avoid saving social media login credentials, customer information and autofill retrieval. If you do online banking for your business, consider having a dedicated device which is used only for online banking and make sure to disconnect it from the network when it is not in use.	
3-5	**Enable remote wiping on your mobile devices**	👤 👥
	Mobile devices normally come with a feature for remotely wiping all content in case the user lost his/her device. Activate that feature and ask employees to promptly report any missing business mobile device as soon as possible so that the device can be recovered, locked out or remotely wiped. This will prevent attackers from accessing your e-commerce systems and accounts.	

	4. Guard Your Social Media Accounts Used in E-commerce	Scope of Applicability
4-1	**Exercise safe behavior on social media**	👤 👥
	Take extra care while using social networking apps and websites. When communicating through social media, be suspicious of any messages that ask for sensitive business information. Social networking sites are becoming an increasingly popular way for attackers to try to get your business information. Assign someone to be mainly responsible for your e-commerce social media accounts.	
4-2	**Get your social media accounts verified**	👤 👥
	Consider getting your social media account verified. Most social media platforms offer a visible indication (e.g., icon next to profile username) to show that this account is verified. Getting verified is a way to increase the customers’ confidence in this account. Online review platforms (such as Ma’aroof 4) are a good way to get verified as well. Be careful of connection requests from other businesses you do not know. You may do a quick online search of the entity to make sure they are legitimate. Avoid linking your social media account to unknown services or apps, and revoke any unnecessary access.	

[4] https://maroof.sa/

	5. Defend Your Network	Scope of Applicability
5-1	**Disable unnecessary services on systems**	👤 👥
	Many devices such as computers and wireless routers come with extra services and features which are often not used. Similarly, many operating systems and apps have extra and unnecessary services and software programs pre-installed. Disable or turn off these features and services.	
5-2	**Segment and segregate networks**	👥
	Divide your network into sub-networks to protect sensitive information from flowing within the non-secure parts of your e-commerce network.	
5-3	**Defend network perimeter**	👥
	Use Intrusion Prevention Systems (IPS) in order to defend your network perimeter. These systems can detect unusual data traffic patterns or anomalies in network activities which may indicate that someone is trying to attack your systems. Another recommended way to defend your network is to implement a firewall in your network. Make sure to review the access list periodically.	
5-4	**Test your systems regularly**	👥
	Conduct penetration tests on your e-commerce systems regularly and anytime you have a major code change or a system upgrade. Penetration testing simulates a cyber-attack such as a DDoS to identify weaknesses in the tested system.	

	6. Continuously Educate and Train Your Employees	Scope of Applicability
6-1	**Develop and implement cybersecurity and privacy policies**	👥
	Develop and implement a cybersecurity policy that defines what employees can and cannot do when using business systems. The policy should highlight the consequences that employees will face in case of violating this policy. Consider training your employees periodically on the cybersecurity requirements highlighted in your cybersecurity policy. Also, consider developing a privacy policy that is based on internationally accepted privacy	

	principles. Make sure to publish a privacy notice that refers to this policy on your e-commerce store to communicate to consumers your commitment to protecting their privacy and their personal data.	
6-2	**Protect against phishing and social engineering**	👥
	Educate your employees and protect against phishing and social engineering. Social engineering refers to psychological manipulation of people into revealing confidential personal and financial information. Attackers usually use phishing emails to conduct social engineering attacks and gather the information they need to commit fraud or gain access to business computer systems or social media accounts. You should educate your employees on the common signs of phishing emails that include, for example: • Poor spelling, grammar and punctuation. • Instead of addressing a specific person, they refer to 'friend' or 'valued colleague'. • Sense of urgency, in terms of time or request from a senior person in the company. • May offer a great discount on a popular item.	
6-3	**Restrict staff from downloading unknown applications**	👥
	Unknown applications are one of the most likely sources of malware. Train employees to only use software that is necessary for business and to download that from trusted sources (e.g., app stores, vendor's official website).	
6-4	**Recognize signs of compromise and how to handle incidents**	👤 👥
	Train employees to handle incidents and recognize signs of compromise. Also train employees on reporting cybersecurity incidents immediately. Typical signs may include: • Computer, applications or network will respond very slowly to commands and requests. • Locked out of key accounts and receiving messages that your password has been changed when you did not change it. • Unable to access your files, applications or services.	

	7. Strengthen Your Internal E-commerce Infrastructure	Scope of Applicability
7-1	**Keep your backup in a secure location**	👥
	If you are using external hard drives for backup, keep these external backup media in a secure location, either in a small fire-resistant safe or preferably in a different building.	
7-2	**Implement a spam filter**	👤 👥
	Implement a spam filter on your email exchange. A spam filter will block most spam and only allow legitimate and acceptable emails to get to your e-commerce business. Refrain from opening links in emails sent by your consumers as these may lead to malicious websites or applications. Also, keep your employees' emails addresses confidential and use generic email addresses (e.g., help@companyname.com) for information posted publicly.	
7-3	**Review audit trails and security logs**	👥
	Continuously monitor and frequently review audit trails and security logs. Audit trails and security event logs (e.g., logs that contain records of login/logout activity) aid in the detection and investigation of cyberattacks. The audits trails will show who accessed the IT systems and what operations were performed. Maintaining proper audit trails and security logs will also help in recovering lost transactions, highlighting security weaknesses and potential points of illegal intrusion for your e-commerce business.	
7-4	**Use email activation and captcha for user registration**	👥
	To avoid mass registrations done by spam campaigns, require users to confirm registrations through clicking a confirmation link in their email or using a CAPTCHA field (online test used to determine whether or not the user is human). The key is to make the confirmation link process easy to follow (email could arrive promptly, setting a timeout, etc.) and the CAPTCHA challenge simple enough for legitimate users not to get frustrated.	

7-5	**Utilize fraud prevention software**	👥
	Utilize an e-commerce anti-fraud software solution as this is considered a good way to stop attacks such as click fraud, mass registration and inventory abuse. Several vendors offer solutions that combine a click fraud or mass registration detection algorithm with a blacklist of known fraudulent IP addresses.	
7-6	**Choose a secure e-commerce platform**	👤 👥
	When looking for the right e-commerce website or business payments platform, choose trusted and reputable companies that have good reviews and are transparent about their privacy policy. Look for international vendors which comply with ISO or PCI standards or local vendors who adhere to cybersecurity standards issued by local regulators (e.g., NCA, SAMA). Similarly, secure payment gateways come with security features such as payment authentication systems (e.g., Verified by Visa) and fraud profiling services, which can check IP addresses, names and previous purchases, to understand if a purchase is legitimate. You should also proactively review the breach notification requirements and liability protections provided with the payment gateway in case of cyberattacks.	
7-7	**Create a customized user registration**	👥
	If you are going to allow users to register on your website, create a customized form and link. Malicious bots (a software application that runs automated tasks over the Internet) are generally programmed to go looking for default links or input parameters to register fake users. Many e-commerce platforms offer customization feature to avoid being detected by bots.	
7-8	**Protect against denial of inventory**	👤 👥
	Denial of inventory is a serious problem in which bots can hold items from a limited inventory, but never actually purchase them, thus denying the goods to other legitimate consumers. Reduce the threat of denial of inventory by, for example, applying shopping cart policies, where you limit the absolute time during which users can hold items or restricting the amount of times they can add the item back to cart.	

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.
CAPTCHA	Acronym for *Completely Automated Public Turing test to tell Computers and Humans Apart* - a computer program or system intended to distinguish human from machine input, typically as a way of thwarting spam and automated extraction of data from websites.
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).
Incident	A compromise through violation of cybersecurity policies, acceptable use policies, practices incident or cybersecurity controls or requirements.

Malware	A program that infects systems, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
Multifactor Authentication (MFA)	A security feature that verifies user identity, which requires the use of several separate elements of identity verification mechanisms. Verification mechanisms include several elements: • Knowledge (something only the user knows "like password"). • Possession (something only owned by the user "such as a program, device generating random numbers or SMS" for login records, which are called: One-Time-Password). • Inherent Characteristics (a characteristic of the user only, such as fingerprint).
Online Backup	A method of storage in which the backup is regularly taken on a remote server over a network, (either within the organization's network or hosted by a service provider).
Patch	Supporting data pack used to upgrade, fix or improve computer operating systems, software or applications. This includes fixing security vulnerabilities and other bugs, with such patches usually called fixes or bug fixes and system usability or performance improvement.
Privacy	Freedom from unauthorized interference or disclosure of personal information about an individual.
SME (Small and Medium Enterprises)	Companies with 6 to 249 employees and SAR 3m to 200m in revenues.
SoHo (Small Office / Home Office)	Individual sellers / companies with 1 to 5 employees, and less than SAR 3m in revenues.
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