



المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

Small Business Handbook

This guide is created to assist small businesses in defending themselves against the most common cyber-attacks.



Is your business ready for a **?**
Cyber Attack **■**

Contents

01	Protecting your data with passwords	01
02	Backing up your data/information	02
03	Prevention against Malware	03
04	Phishing attacks and how to avoid them	04
05	Safeguarding your smartphones (and tablets)	05
06	Collect security logs	06



Protecting your data with passwords

- Avoid using passwords that are easy to guess (such as family and pet names or birthdates). Bear in mind not every complex passwords offers protection because they are widely known like P@ssw0rd or Abc@123.
- If you suspect someone else knows your password or notice any suspicious activity on your account, change your password immediately or notify the person concerned.
- Always use two factor authentication (2FA) on all your accounts.
- When setting up new devices (eg. Routers, biometrics etc) in your business and before providing access to your employees, make sure to change the default passwords set by the manufacturers.
- Consider using a password manager, which are programs that generate and store passwords for you and give you access to them through a master password. Because the master password protects all your other passwords so don't forget to make it a strong one and never use old passwords (compromised/breached) for master passwords.
- For better protection of customer data make sure to use encryption products on laptops and PCs wherein this data resides for daily operation.



Backing up your data / information

- **Make regular backups of your critical information and verify that it can be restored. This will lessen the impact of data loss due to theft, fire, or other physical damage, as well as ransomware.**
- To ensure customer/critical data stay safe and untampered, encrypting backup/disk is advisable.
- Determine what should be backed up. Documents, photos, emails, contacts, and calendars are typically kept in a few common folders. Make backups a regular part of your routine by turning on automatic backups.
- Unplug your USB connected hard drive from your devices when not performing a backup.



Prevention against Malware

By implementing the following, you can protect your company from the damage caused by 'malware'

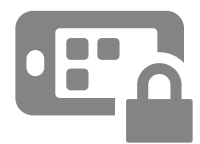
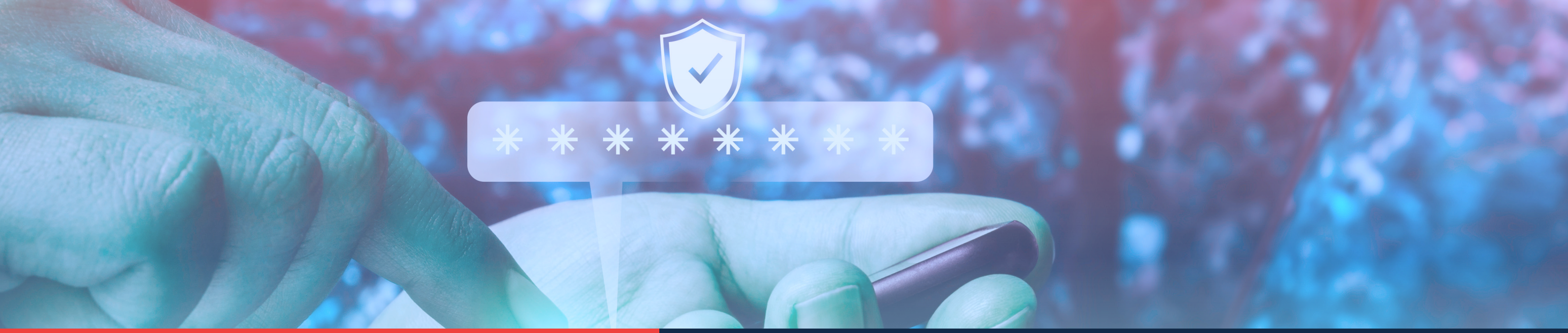
- Trusted Antivirus software should be installed on all servers , computers & laptops. On tablets and smartphones, only approved software should be installed, and users should avoid downloading third-party apps from unknown sources. By implementing the following, you can protect your company from the damage caused by 'malware'
- Make sure to update Operating system and Application software & use the 'automatically update' option.
- Access to removable media such as SD cards and USB sticks can be restricted on computers and servers. Use a safer method to exchange files and folders and apply the needed security measures.
- Unless there is no firewall provided by your antivirus or installed on your network make sure to keep your operating system's firewall "ON" as it acts as a barrier between your system and harmful communications.



Phishing attacks and how to avoid them

The attack vector for carrying out phishing attacks include social engineering (through emails, social media, and SMS). The scamming methods are repeated but the attackers are getting craftier when sending fake documents, emails body and attachments , instructions that look like the original .

- If you suspect a successful attack, scan for malware and change passwords as soon as possible. Encourage your employees to report cyber incidents or suspicious activities.
- Look for possible signs of phishing, such as poor spelling and grammar or low-resolution versions of well-known logos. Verify if the sender's email address is genuine or if it is attempting to impersonate someone you know.
- Configure your staff accounts using principle of " least privilege ". Limit administrator privileges to one or two accounts and supervise the activities.



Safeguarding your smartphones (and tablets)

- Activate mobile device PIN/password protection/fingerprint recognition.
- Configure devices so that they can be tracked, remotely wiped, or remotely locked if they are lost or stolen.
- Keep your devices (and all installed apps) up to date and use the 'automatically update' option.
- Use mobile hotspots instead of public Wi-Fi when sending/receiving sensitive data.
- Never click on any links received by suspicious senders on social messaging or via suspicious emails or adware popups whilst surfing the internet.



Collect security logs

- If you are outsourcing your IT service or you are in contact with a support team for your IT Infrastructure, make sure to ask for periodical security monitoring or collection of logs from devices (computer/firewall). That will be helpful when an incident occurs — for example, if you've had multiple failed logons to your network from suspicious IP Addresses.

WITH REGARDS
NATIONAL CYBER SECURITY CENTER



www.ncsc.gov.bh
#CyberWiser

