enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

NATIONAL CYBERSECURITY ALLIANCE

STAY SECURE ONLINE – 2020 TRANSATLANTIC CYBERSECURITY CHECKLIST FOR SMALL BUSINESSES

INTRODUCTION

Small businesses are an important driver for innovation and growth for the European Union and for the United States of America. They are also the staple for both economies and their workforces. The COVID-19 outbreak has put an incredible stress on these businesses this year. Many are struggling to grasp a new way of doing business in today's hyper-connected world. For those small businesses navigating this new digital environment where employees work from home and business is increasingly conducted online, cybersecurity has become an increased concern.

This **'Stay Secure Online – 2020 Transatlantic Cybersecurity Checklist for Small Businesses'** has been drafted jointly by the European Union Agency for Cybersecurity (ENISA) and the National Cyber Security Alliance (NCSA). This document identifies many of the challenges faced by small businesses during this year's digital surge and offers small business owners a basic guide to maintaining digital security.

CYBERSECURITY CHALLENGES FACING EU'S AND USA'S SMALL BUSINESSES

The EU Agency for Cybersecurity and the National Cyber Security Alliance have identified four main cybersecurity challenges faced by small businesses (referred to as Small and Medium Enterprises – SMEs - in Europe) across the European Union and United States of America this year, fuelled by the COVID-19 pandemic as the below:

Low Cyber-Awareness: Cybersecurity may be a complex issue connected with technical solutions and measures, but it must be a part of the culture for small businesses as a successful cyber-attack can cause serious financial and/or reputational harm to any size of business.

Lack of Remote IT Security: As more employees log in to their home computers to work, more data and communications are being transmitted across insecure channels - ultimately leaving valuable business content exposed.

High Cost of Cybersecurity Solutions: The cost of technical solutions, organisational overhead, cybersecurity trainings and cybersecurity expertise require funds that many businesses simply do not have.

Increased Attacks such as Phishing: Teleworking has opened new opportunities for cyber criminals through 'urgent' and 'fear-based' emails to trick online users into revealing personal information, click on malicious links or attachments, and inadvertently download malware directly on their computers.

2020 TRANSATLANTIC CYBERSECURITY CHECKLIST FOR SMALL BUSINESSES

This 2020 Transatlantic Cybersecurity Checklist for Small Businesses provides baseline tasks that small business owners can do to gain peace of mind that their businesses, information and employees are more secure online.

□ **Create a digital mind-set based on the BIG FOUR: Strong passwords. Antivirus. Automatic updates. Backups.**

□ **Educate employees on cyber hygiene basics:**

- Never leave your laptop unattended and always lock your device when not in use;
- Never plug in an unknown USB drive or other device into your computer;
- Store company passwords securely as advised by your employer;
- Avoid emails from unknown sources that call for 'urgent' action;
- Check links before clicking on them, each and every time;
- Back up data on a regular basis and check up on saved data;
- Install anti-spam, anti-spyware and anti-virus software, and make sure your operating system is up to date;
- Use your business phone hotspot instead of open Wi-Fi networks when working in public spaces, outside your home or office.

□ **Establish and enforce an IT security policy:** First, you need to assess the main assets of your business and the possible threats, both internal and external. Once you know what you are protecting, you can put a policy into place and appoint a manager to oversee implementation. Each policy should include a **set of rules** that addresses key questions every employee should be able to answer:

- May I access enterprise network from a home computer?
- May I access work email via my private smartphone? If so, what are the requirements?
- May I use software that is unapproved by IT on my work computer?
- May I upload company documents to a public cloud? If so, should I invite specific colleagues to collaborate, or may I to share the documents through a link?
- May I use public Wi-Fi at an airport or in a hotel? May I use such a network to access my work email?
- May I use a password manager? If so, which one?

□ **Ensure regular backups and updates:** Establish an automated system for you and your employees to backup data on a regular basis. This will prepare you for facing attacks such as ransomware. Schedule regular updates for your company servers, workstations and smartphones. Apply all the official recommended updates.

□ **Secure remote access:** If you are not operating your business on the cloud, and are instead operating your own ICT environment, make sure to secure the remote access as much as possible. You can do this by using a virtual private network (VPN), encrypting communications, enforcing strong passwords, setting up Multi-Factor Authentication (MFA) where applicable, and, most importantly, by giving your employees clear guidelines and access to help.

□ **Create a secure meeting space:** Allow your employees to use digital communications such as chat, audio, video and screen sharing in a secure manner by requiring them to follow good practices such as:

- Use password protection for all meetings;
- Keep conference links and meeting passwords within the invited participant list;
- When using video, ensure your visual background does not reveal personal or professional data to participants.

□ **Make an incident management plan:** Be prepared with a plan that lays out how to handle cyber incidents, provides local resources that can help and includes a response policy for your internal and external audiences. Then exercise it to see whether it works in real life.