UNDER
DEFENSE

# 10 Basic Tips

## to make yourself and organization more secure

1. Use **modern operating systems** that have a serious level of protection against malicious programs (Windows 10, Newest Mac OS). Advise with UnderDefense IT Team*;*

2. Constantly **update** your Operating Systems, Applications and other programs you may use. Download these systems, apps and their updates **ONLY** from the official sites of the OS developer or official websites and stores (apple store, google play market, etc). If there is an automatic update mode, TURN IT ON!
*Every update of any system or application has security check and patches to prevent you from being breached or hacked;*

3. **Limit physical access** to the computer for other people. LOCK your screen at ALL TIMES when you're away from the desk (Windows OS - keyboard key - “win+L”; MacOS - shift+ctrl+power button);

4. Use external storage media, such as a flash drive, disk or file from the Internet, only from **trusted sources** (OneDrive from Windows, Google Cloud, Amazon Cloud Services, Apple Cloud);

5. Do not open computer files obtained from **unreliable sources**. Even those files that your friend sent. It's better to double check with your friend if he or she sent them to you ;

6. Do **not share** your sensitive information through public Wi-Fi networks. Working in such networks, it is also desirable NOT TO ENTER access passwords, logins, credit card numbers, ID, etc;

7. Use only a secure connection over **HTTPS**, rather than HTTP, i.e. when typing a web address, enter “**https: //**”; install extension such as“https everywhere” to be more secure;

8. Use **MFA**(Multi Factor Authentication ) In case of compromising your password **MFA** will help to keep access to your corporate data safe.

9. Choose a **complex password**. Criminals will not just guess the **complex password**. Strong passwords are passwords that contain at least 8 characters and include lowercase and uppercase letters, numbers and a few characters, such as a dollar sign or exclamation mark, etc. For example,
$ tR0ng! ; *For more details please refer to Symphony Solutions Password Policy.*
• **USE PASSWORD MANAGERS!** (1Password, Dashlane: #1, KeyPass)
• **Regularly Change your password.**

10. Nothing is really **free**. Be careful, because when you're offered free content, some paid services or viruses might be hidden in there.