

General Recommendations - Protect Your Business IT - August 2023

We live with a threat scenario, that changes rapidly. What was safe yesterday might be at risk today.

You better start getting some new habits, that will help staying ahead of the risks 😊



KAJE
ENGINEERING
INTELLIGENT FLOW SOLUTIONS

KAJE ApS
EGESKOVVEJ 8
DK-3490 KVISTGAARD
WWW.KAJE.EU
EMAIL: HELLO@KAJE.EU
+45 3064 3569

CVR/SE :DK36424389

End-user

- Unique logins and passwords for each account
- Unique passwords with a minimum length of 20 characters - some are even talking about 30 not being enough - created by using a combination of letters (a-z, A-Z) and digits (0-9) plus a few Special Characters (Pure Mathematics).
You can alternatively use a sentence from a poem or book of your preference – just remember to add digits and special characters then.
- **Use a verified Password Manager** - check online as there are plenty of "Fake" products in the APP Stores. We recommend **Sticky Password**. [<https://kaje.eu/sticky-password>]
- **Use 2FA (2 Factor Authentication) wherever it's an option.** We recommend **Authy**. [<https://authy.com/>]
- **Always pay attention to the naming of the link in an email, text, website, etc.**
- Separate private use from business use
- Free offerings have a cost - it's your personal data...
- Use more than one browser and separate the use. Example: Brave (or Mozilla Firefox) for logins where vital information is exchanged, Vivaldi for SoMe, Opera for Streaming Services and LibreWolf for less sharing of personal protection when surfing online.
- **Never save your login details in the browser**
- Make the **Ecosia Search engine** [<https://www.ecosia.org/>] your preferred one in all browsers (You support planting trees 😊)
- Get the habit of **shutting down** your computer by the end of the day – **all your login details are stored in the memory until a reboot or shutdown has been executed.**
Nowadays this is enough for a hacker to gain access to any of your accounts.

Computer (Microsoft Windows)

- **Create a default user without admin rights for your daily use**
- Only login with your admin account if Windows requires it
- Remember to check for updates frequently
- Use a **licensed** Anti-Virus application (3rd party) that protects your data both on the device and while using the Internet services. We recommend **AVAST** or **Heimdal**[®] (Contact us for a talk regarding which one to choose).
- **Be careful with free software** - remember to check online if there is any risk associated with the one you are looking at

Disclaimer: All information, software, services, and comments provided are for informational and self-help purposes only and are not intended to be a substitute for professional legal advice.

General Recommendations - Protect Your Business IT - August 2023

We live with a threat scenario, that changes rapidly. What was safe yesterday might be at risk today.

You better start getting some new habits, that will help staying ahead of the risks 😊



KAJE
ENGINEERING
INTELLIGENT FLOW SOLUTIONS

KAJE ApS
EGESKOVVEJ 8
DK-3490 KVISTGAARD
WWW.KAJE.EU
EMAIL: HELLO@KAJE.EU
+45 3064 3569
CVR/SE :DK36424389

Computer (MAC)

- **Create a default user without admin rights for your daily use**
- Only login with your admin account if Mac iOS requires it
- Remember to check for updates frequently
- **Get a new habit of booting your device once every day** (some patches require a restart to be installed)
- Use a **licensed** Anti-Virus application (3rd party) for scanning what Apple allows others to do, like your emails and online traffic. We recommend **AVAST** or **Heimdal**[®].
- **Be careful which APPS you download from the store** - remember to check online if there is any risk associated with the one you are looking at.

Smartphone & Tablets (iPhone/ Android)

- Free offerings have a cost - it's your personal data...
- **Be careful which APPS you download from the store** - remember to check online if there is any risk associated with the one you are looking at
- Use a **licensed** Anti-Virus application (3rd party) for scanning your device, applications and online traffic. We recommend **AVAST** (iPhone/ Android) - however they only have a consumer version for this kind of devices or **Heimdal**[®] (only Android)
- **Get the habit of verifying that your Anti-Virus application is active** after an update – it turns out that Google often de-activate third-parties Anti-Virus during the update sequence (Experienced with several vendors).
- **Get the habit of rebooting your phone once every week** 😊

Your data

- Your data is stored using technology that can fail - either due to lack of connectivity, being hacked or hardware failure, so the old rule: "store your data at three different medias" continues to be worth following
- Recommend you to do a monthly "file copy" of your data to an external USB drive, that you disconnect and put a side in a safe place
- Protect your online share with a strong unique password **and** 2FA

NAS Drives/ USB Drives

- Easy to install - some includes Backup features/ application
- Be aware of that some NAS drives connects automatically to the Internet without any option to block for this opening. The risk here is that if the vendor is hacked, then your account equals your data will be open for access.
- Your data is stored using technology that can fail - either due to lack of connectivity, being hacked or hardware failure – use it with care

Disclaimer: All information, software, services, and comments provided are for informational and self-help purposes only and are not intended to be a substitute for professional legal advice.

General Recommendations - Protect Your Business IT - August 2023

We live with a threat scenario, that changes rapidly. What was safe yesterday might be at risk today.

You better start getting some new habits, that will help staying ahead of the risks 😊



KAJE
ENGINEERING
INTELLIGENT FLOW SOLUTIONS

KAJE ApS
EGESKOVVEJ 8
DK-3490 KVISTGAARD
WWW.KAJE.EU
EMAIL: HELLO@KAJE.EU
+45 3064 3569

CVR/SE :DK36424389

Documentation

- Remember that data online might not be available when you need them
- Always keep track of the services you use for your business data, i.e. create a simple document that you easily can maintain
- Download and print the agreements related to the services used
- Remember that local regulations related to accounting might be different from the local & global regulations covering requirements related to Data Protection

Cloud Share Services

- Be aware of which data you store as some might have to be GDPR compliant (or similar related to Data Protection & Privacy Regulations)
- Shared responsibility means that your vendor secures the backend, but you are in control of who has access to your data
- Requires connectivity in order to work as intended when it comes to speed
 - a poor connection will influence the synchronization between your device and the service being used
 - an attack to the infrastructure might disconnect you from the service

Disclaimer: All information, software, services, and comments provided are for informational and self-help purposes only and are not intended to be a substitute for professional legal advice.

General Recommendations - Protect Your Business IT - August 2023

We live with a threat scenario, that changes rapidly. What was safe yesterday might be at risk today.

You better start getting some new habits, that will help staying ahead of the risks 😊



KAJE
ENGINEERING
INTELLIGENT FLOW SOLUTIONS

KAJE ApS
EGESKOVVEJ 8
DK-3490 KVISTGAARD
WWW.KAJE.EU
EMAIL: HELLO@KAJE.EU
+45 3064 3569
CVR/SE :DK36424389

Some other “nerdy” comments

- The hardware configuration:
 - For business use it's our experience that an Intel Core i5 or Core i7 is what you will need when it comes to performance and stability.
- The operating system aka OS:
 - Since 2021 there seems to be a stronger relation between hardware components and OS performance not to mention potential security issues – so give it second thought before upgrading your old computer to newest OS generation.
 - Windows is known for having issues – the positive part is that they (and AV vendors) are working to secure all gaps as soon as they are reported.
 - Microsoft has given the AV vendors access to let their AV applications operate at the OS layer => providing the user with a better integrated security
 - Apple has not yet given the AV vendors full access to their OS. This leaves a risk for the user if forgetting to update frequently. Apple claims their OS is secure, but we have seen and continue to see bugs in the MacOS...
 - Android is an open-source OS developed by Google. Very few vendors stick to use the basic core in their products as they have the option to modify or add additional features.
 - Linux is an open-source OS available in several version's aka Distro's for free. Linux has a reputation of being for nerds, but a distro like **Linux Mint** [<https://linuxmint.com/>] includes what you need of applications and is easy to setup. You can also buy a subscription at a vendor, where the default version is primed with additional features and will be maintained forwards.
- Applications:
 - **Spend some time on evaluating your needs vs nice-to-have.** The more advanced features, the more you put yourself at risk in terms of privacy or security.
 - Recommend to un-install any applications you're not using.
 - Unless you are hooked up to a company system your needs will be fulfilled using an email client like **Thunderbird** [<https://www.thunderbird.net/>] and for documents and presentations like **Libre Office**. [<https://www.libreoffice.org/>]
- Anti-Virus & Firewall:
 - Free versions are better than none (using trusted vendors)
 - Paid subscriptions are required if you care about your data
 - Consumer version are just for personal use
 - Professional versions are needed in the event you work with business data
 - Evaluate your need vs nice-to-have – **the content in the subscription package is more relevant than the price tag when it comes to protecting your data**

Disclaimer: All information, software, services, and comments provided are for informational and self-help purposes only and are not intended to be a substitute for professional legal advice.