Safe browsing habits for employees at work & home wifi

DO's

☐ Use trusted paths

- Access websites via **bookmarks** or official links, not forwarded or unknown ones.
- Verify the **URL**: spelling, domain, and "https://" before entering credentials.

☐ Protect your credentials

- Use **strong, unique passwords and multi-factor authentication (MFA)**.
- Only enter passwords on legitimate company or known partner sites.

☐ Stay secure while browsing

- Ensure that **Internet Security Tool** provided from your company is **active**.
- Keep your **browser & security tools** updated and active.
- Connect through **secure Wi-Fi (WPA2/WPA3)** and VPN when required.
- Close browser sessions after sensitive activity (e.g., banking, HR portals).

☐ Think before you click

- Be cautious with ads, pop-ups, free downloads, and "too good to be true" offers.
- Report suspicious sites, links, or requests to IT/security.

Atos

Safe browsing habits for employees at work & home wifi

DONT's

☐ Do not

- Don't click **on unexpected links** in emails, chats, or ads.
- Don't enter credentials into **unfamiliar or redirected websites**.
- Don't download **unverified extensions, plug-ins, or free software.**
- Don't ignore **browser or security warnings**.
- Don't use **public Wi-Fi without VPN** for company work.

RISK's

☐ Be aware of

- **Phishing & Spoofed Sites** stealing credentials.
- **Malware** hidden in downloads or browser extensions.
- **Data Theft** from weak Wi-Fi or careless browsing.
- **Deepfake / Voice Spoofing** used to trick you into sharing sensitive info.

Atos