Cybersecurity – Covid19

Increased risk during the pandemic event

Essential recommendations

- **Be safe:** Please observe social distancing & listen to your country recommendations
- **Do not entrust your PC to any 3rd parties:** any person having access to you PC can use your identity!
- **Never give out your credentials:** To anyone! No exception!
- **Use strong passwords**: avoid dictionary words and easily guessable passwords
- **Clean user databases:** remove or disable user accounts of former associates or external contractors that left the company.
- **Strictly limit the administrative rights** to only duly authorized people.
- **Patch your systems thoroughly**, especially those exposed to the Internet

How to avoid Phishing

- **Avoid clicking on links in unsolicited emails** and be wary of email attachments.
- **Be careful of "fake emails":** emails with displayed sender name not matching the email address (e.g.: CEO Name <smtp-zeus@gmail.com>)
- **Do not reveal personal or financial information in email**, and do not respond to email solicitations for this information.
- **Use trusted sources** — such as legitimate, government websites — for up-to-date, fact-based information about COVID-19.

Strictly follow those guidelines

- **Use VPN connections** to remotely connect to your infrastructures if technically possible.
- **Do not use any other email solutions or unauthorized software** while working from home.

Report any incidents

- **Please report any incidents** that you may experience, sharing these incidents can be beneficial to all our OpCos.

Management des Risques et des Assurances de l'Entreprise
80 BOULEVARD HAUSSMANN 75008 PARIS - TEL : +33 (0)1 42 89 33 16 - FAX : +33 (0)1 42 89 33 14 - amrae@amrae.fr - www.amrae.fr