Управлявайте добре цифровия риск по време на професионални пътувания и дистанционна работа!

Практиките на дистанционна работа, работа на обществени места или в обществения транспорт, могат да породят проблеми с безопасността. Опасности при дистанционна работа:

- шпиониране на вашата чувствителна информация, прихващане на вашето оборудване, кражба на вашето оборудване, вашата лична информация и връзки.

Осведомете служителите си за правилните мерки:

- Архивирайте редовно данните си.
- Предпочитайте методите за удостоверяване, при които паролите не са предварително записани във вашето оборудване.
- Криптирайте вашите най-чувствителни данни или целия твърд диск. Не забравяйте да конфигурирате парола за спешно дешифриране.
- Ако някога ви се наложи да отсъствате, винаги заключвайте вашето оборудване или дори го изключете. Конфигурирайте продължителност за автоматично заключване по-малко от 5 минути.
- Не свързвайте вашето професионално оборудване към оборудване, на което нямате доверие.
- Откажете свързването на оборудване, принадлежащо на трети страни (смартфон, USB флаш и др.).

- Ако трябва да презаредите мобилния си телефон, не го свързвайте към компютър на трета страна или USB контакт за самообслужване, а използвайте собствено електрическо зарядно устройство.
- Не свързвайте вашите работни станции към публични интернет мрежи (магазини, хотели и др.).
- Ако трябва да обмените документи с трета страна, предпочитайте обмен по имейл или използвайте предназначена USB флашка само за тази цел.
- Бъдете бдителни относно поверителността на обмена по време на вашите телефонни разговори и видеоконференции.
- Използвайте само хардуер (компютър, лаптоп, телефон) предоставени от фирмата. Забранете използването на лични устройства и лични имейл адреси за професионални нужди.
- В случай че имате нужда от дистанционен достъп до информационни системи на компанията, планирайте инсталирането на софтуер за връзка с VPN криптиране (виртуална частна мрежа).
- Не разкривайте директно чувствителни бизнес приложения или данни в интернет (разрешете достъп до тях само през VPN).
- Защитете достъпа до базова входно-изходна система със стабилна парола и активирайте функцията за защитено зареждане на вашите работни станции.