UPPSALA
UNIVERSITET

Resesäkerhet – vad ska jag tänka på?

- Ta bara med dig den information du behöver på resan.
- Fundera över hur du skyddar den information du tar med dig. Är den säkerhetskopierad? Krypterad? Information som här lagras i en säker lagringslösning kan utsättas för stora risker om du kopierar över den till en mobil enhet som du tar med dig på resan.

- Ta bara med de enheter som du verkligen behöver
- Vid resor utanför EU - lämna om möjligt din dator hemma och ta med en lånedator.

Övrigt att tänka på inför resan

- Kolla med resebyrån, UD, och ev kollegor som besökt landet nyligen, om det finns regler/restriktioner för information lagrad elektroniskt (t.ex. om datorns disk får vara krypterad)
- Har du tillgång till universitetets VPN-tjänst? Instruktioner finns i Medarbetarportalen.
- Är programvara och appar uppdaterade?
- Har enheterna automatisk låsning, lösenord/PIN-kod?

Under resan

- Håll koll på dina enheter och var uppmärksam på din omgivning.
- Använd sekretessfilter på skärmen så inte andra ser vad du gör – undvik ”visual hacking”.
- Använd Eduroam där det finns.
- Koppla inte upp dina enheter mot publika öppna WiFi-nät.
- Även anslutning till lösenordsskyddade nätverk, exempelvis på hotell, kan medföra stora risker. Var kritiskt inställd till frågor som ställs i samband med anslutning till nätverket.
- Använd universitetets VPN-tjänst för att nå dina resurser vid universitetet.
- Avaktivera bluetooth och positionstjänster du inte behöver under resan.
- Ta med egna USB-minnen - använd inte gratis USB-minnen (t.ex. från mässor).
- Använd din egen laddare – minska risken att något händer. Fel laddare kan skada dina enheter och laddare riggade med skadlig kod förekommer.

Efter resan

- Kör en viruskoll på de enheter – även USB-minnen – du haft med dig på resan.
- Var uppmärksam på eventuella phishing-försök som kan ha koppling till din utlandsvistelse.
- Om du är misstänksam eller funderar över något – kontakta säkerhetsavdelningen (security@uu.se).

Se våra webbaserade kurser för fler tips: Informationssäkerhet, resesäkerhet, IT-säkerhet

UPPSALA
UNIVERSITET

IT travel security – what do I need to consider?

- Bring only the information you actually need during your travel.
- Think about how you will protect the information you will bring. Do you have backups? Is it encrypted? Information stpred securely at the office may be subjected to risks when copied to a mobile device and brought abroad.
- Only bring devices (laptop, cell phone etc) you really need.
- If travelling outside the EU – if possible leave your computer at home and bring a loaner device.

Other things to consider before travelling

- Check with the travel agency, Ministry of Foreign affairs, and any colleagues who recently visited the country in question, if there are any restrictions for bringing information electronically (i.e. may the computer disk be encrypted)
- Do you have access the the university VPN service? Instructions can be found at Medarbetarportalen.
- Are apps and software updated?
- Do all units have automatic screen lock, password/PIN-codes?

During the travel

- Keep tabs on your devices and pay attention to your surroundings.
- Use a privacy filter on your screen so others cannot see your information – avoid visual hacking.
- Use Eduroam wherever possible.
- Do not connect your devices to public unprotected WiFi networks.
- Even connecting to a password protected network, in hotels or conference areas, may be risky. Be critical to questions popping up when you connect.
- Use the university VPN service to reach resources at the university.
- Deactivate bluetooth and position services you do not need when travelling.
- Bring your own USB stick if needed – do not use free USB sticks from conferences etc.
- Use your own charger to lessen the risks. Wrong type of charger (or a pirate version) can damage your unit or even cause a fire. Also there are known cases of chargers rigged with malware.

After the travel

- Run a virus scan on the devices – including USB – that you brought with you abroad.
- Be aware regarding potential phishing attempts related to your trip.
- If you have any suspicions or questions – kontakt the Security and safety division (security@uu.se).

See also our web based courses for more information: Information security, travel security, IT security