Sicheres Surfen im Internet

1. *Überprüfe bestehender Datenlecks*
   Über Identity Leak Checker (https://haveibeenpwned.com/) kann herausgefunden werden, ob zu einem E-Mail-Konto gehörige Informationen und Passwörter bereits in einem bekannten Hack enthalten sind. Ist dies der Fall, ändern Sie bitte Ihre geleakten Passwörter.

2. *Verschlüsselung verwenden*
   Die meisten Webseiten bieten heute an, dass man mit ihnen sicher verschlüsselt über den Einsatz des HTTPS-Protokolls kommuniziert. Surfen Sie unsichere Webseiten nicht an.

3. *Clever klicken*
   Online-Betrug kann teuer werden. Bleiben Sie wachsam und lassen Sie sich Zeit. Im Zweifelsfall besser nicht anklicken.

4. *Sorgfältiger Umgang mit persönlichen Daten*
   Je mehr persönliche Daten Sie im Internet preisgeben, um so attraktiver und ggf. auch lukrativer werden Sie für Cyberkriminelle. Geben Sie also nur die nötigsten Informationen preis, falls erforderlich.

5. *Starke Passwörter benutzen*
   Ein starkes Passwort ist mindestens 15 Zeichen lang und besteht aus Zahlen, großen und kleinen Buchstaben sowie Sonderzeichen. Nutzen Sie bitte keine vollständigen Wörter. Für verschiedene Zwecke (Konten) sollten verschiedene Passwörter benutzt werden.

6. *Verwende Zwei-Faktor-Authentifizierung*
   Zwei-Faktor-Authentifizierung ist viel sicherer als ein einfaches Passwort, da es dann nicht mehr ausreicht, ein solches abzufangen, um illegal in ein System zu kommen.

7. *Den Computer schützen*
   Jeder Computer benötigt einen guten Virenscanner und eine Firewall, damit die Gefahr der Infektion mit Schadsoftware laufend überprüft und abgewendet werden kann. Daher sind ein Anti-Virus Programm (Sophos) und eine aktivierte Firewall unbedingt erforderlich.

8. *Regelmäßig Programme aktualisieren*
   Updates schließen Sicherheitslücken in Programmen. Vergewissern Sie sich, dass alle Programme und „Plugins“ immer auf dem letzten Stand sind.

9. *Daten sichern*
   Damit im Ernstfall keine Daten verloren gehen, sollten regelmäßig Sicherungskopien gemacht werden. Aus diesem Grund speichern Sie Ihre Daten auf den Netzlaufwerken der UR ab. Das RZ erstellt regelmäßige Back-ups.