Die 14 Gebote zum Umgang mit IT-Geräten und dem Internet

1. **Seien Sie paranoid und handeln Sie überlegt!**
   Bewegen Sie sich wachsam und mit gesunder Skepsis durch das Internet! Gehen Sie davon aus, dass auch Sie Ziel von Cyberkriminellen werden können! Hören Sie auf Ihre Firewall im Kopf!

2. **Verwenden Sie sichere Passwörter!**
   Mindestens 8 Zeichen, Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen, KEINE nachvollziehbaren oder zu erratenden Daten verwenden (Geburtstage, Name des Haustiers o.ä.)!

3. **Benutzen Sie verschiedene Passwörter!**
   Nutzen Sie NICHT das gleiche Passwort für unterschiedliche Dienste und Funktionen! Das gilt besonders beim Online-Banking oder in sozialen Netzwerken (Stichwort Identitätsdiebstahl)!

4. **Seien Sie sparsam mit Ihren Daten!**
   Veröffentlichen Sie in sozialen Netzwerken nur die allernötigsten Informationen über sich und achten Sie darauf, wer diese einsehen darf!

5. **Installieren Sie Sicherheits- bzw. Softwareupdates möglichst zeitnah!**
   Updates schließen häufig Sicherheitslücken, die früher oder später von Cyberkriminellen ausgenutzt werden!

6. **Öffnen Sie KEINE Links oder Anhänge in E-Mails unbekannter Absender!**
   Diese enthalten nur selten harmlose Informationen!

7. **Prüfen Sie E-Mails bekannter Absender auf Authentizität!**
   Achten Sie auf Schreibfehler in der E-Mail-Adresse oder ungewohnte Formulierungen. Fragen Sie im Zweifelsfall telefonisch nach (besonders wenn die Nachricht Links oder Anhänge enthält)!

8. **Öffnen Sie E-Mail-Anhänge und Downloads nicht direkt!**
   Speichern Sie diese ab und prüfen die Datei mit dem Antivirenprogramm (Rechtsklick → Datei nach Viren und Spyware scannen)

9. **Verwenden Sie Werbe- und Skriptblocker in Ihrem Browser!**
   Werbung auf Webseiten ist nicht nur lästig sondern oft auch ein Einfallstor für Schadsoftware. Skripte im Hintergrund analysieren Ihr Nutzerverhalten, können im schlimmsten Fall jedoch über Sicherheitslücken auch ihr System kompromittieren!

10. **Nutzen Sie KEINE öffentlichen WLAN's!**
    Sie wissen nicht, ob der Betreiber des WLAN-Hotspots vertrauenswürdig ist und ob andere Nutzer nicht versuchen ihre Daten abzufangen und zu manipulieren! Wenn es nicht anders geht, nutzen Sie zumindest eine VPN-Verbindung (z.B. das VPN der TU Dresden)!

11. **Verwenden Sie ein kostenpflichtiges Antivirenprogramm!**
    Kostenpflichtige Programme haben einen größeren Funktionsumfang = mehr Sicherheit!

12. **Aktivieren Sie die Anzeige von Dateiendungen!**
    In Windows ist die Anzeige von Dateiendungen bekannter Dateitypen standardmäßig deaktiviert. Das können Cyberkriminelle ausnutzen um ausführbare Dateien zu tarnen!

13. **Sperren Sie Ihren Bildschirm immer wenn Sie den Raum verlassen!**
    Ein ungesperrtes Gerät ist eine Einladung zur Datenspionage oder zur Installation von Schadprogrammen, z.B. per USB-Stick (unter Windows: ⊞ + L)!

14. **Stecken Sie KEINE unbekannten Geräte an Ihr IT-System!**
    Einen gefundenen USB-Stick, eine USB-Maus oder eine SD-Karte könnte einfach jemand verloren oder liegen gelassen haben. Sie könnten aber auch absichtlich zurück gelassen worden sein, um das System des Finders anzugreifen!