Empfehlungen für IT-Sicherheit an den Schulen in NÖ

1. E-Mails kritisch prüfen

- Bei E-Mails vorsichtig sein, da Urheber von Phishing-Mails seriöse Absender immer besser nachahmen.
- Damit Sie nicht in die Falle tappen, sollten Sie sich Zeit für den 3-Sekunden-Sicherheits-Check nehmen: Prüfen Sie Absender, Betreff und Anhang vor dem Anklicken.
- Um unerwünschte Mitleser/innen auszuschalten, empfiehlt es sich, E-Mails vor dem Versand zu verschlüsseln. Auf diese Weise kann nur der rechtmäßige Empfänger oder die Empfängerin die Nachricht lesen.

2. Verantwortungsvoller Umgang mit Passwörtern

- Notieren Sie Ihre Passwörter keinesfalls auf Zetteln oder Post-its am Monitor, auch nicht an vermeintlich diskreten Stellen wie unter der Tastatur.
- Teilen Sie Ihre Passwörter nicht.
- Nutzen Sie für Ihre Geräte und Anwendungen verschiedene Passwörter und wechseln Sie diese in regelmäßigen Abständen.
- Wählen Sie ein möglichst sicheres Passwort, das sich nicht leicht erraten lässt – also nicht Ihren Geburtstag oder den Namen Ihres Kindes oder Haustiers.

3. Schutz sensibler Daten auf PC, Laptop, etc.

- Sperren Sie den Zugriff auf Ihr Gerät – auch wenn es sich nur um eine kurze Abwesenheit von wenigen Minuten handelt.
- Schließen Sie keine Wechseldatenträger (USB-Sticks) unbekannter Herkunft an Ihren Rechner oder Laptop an. Es besteht die Gefahr einer Infektion mit Schadcode.
- Setzen Sie keine private Hardware im Schulnetz ein und speichern Sie keine Schuldaten auf privaten Datenträgern.
- Nutzen Sie nur die offiziell freigegebene Software auf Ihren Geräten.
- Geben Sie auf USB-Sticks mit Dokumenten acht und schützen Sie diese ggf. ebenfalls mit einem Passwort.

4. Sichere Internetnutzung

- Beschränken Sie die private Internetnutzung in der Schule auf ein Minimum.
- Konfigurieren Sie Ihren Browser so, dass Pop-up-Meldungen unterdrückt werden.
- Achten Sie auf Hinweise bezüglich ungültiger und/oder abgelaufener Sicherheitszertifikate von Web-Diensten.
- Grundsätzlich sollten Sie mit Ihren persönlichen Daten in sozialen Medien vorsichtig umgehen, da Internet-Betrüger auch hier nach Informationen suchen, die sie zum Beispiel für die Gestaltung von unechten E-Mails nutzen.