Victoria Graf

TU Graz expert

EN

Reinfried O. Peter

Bildquelle: Lunghammer – TU Graz

Informationssicherheits-beauftragter der TU Graz

- Seit 37 Jahren an der TU Graz tätig, 30 davon beim Zentralen Informatikdienst – und dort seit 2016 stellvertretender Leiter
- Surft auch privat über eine VPN-Verbindung zur TU Graz, denn diese bietet automatisch besseren Schutz

Aller guten Dinge sind zwei

Ein zweiter Faktor bei der Anmeldung an den IT-Systemen unserer Universität erschwert den unberechtigten Zugriff auf TU Graz-Accounts. Wichtig: Aktivieren Sie zumindest zwei Token für die 2-Faktor-Authentisierung (2FA), z. B. einen auf Ihrem Laptop und einen auf Ihrem Handy. So können Sie weiterhin selbstständig auf Ihren Account zugreifen, wenn einer Ihrer 2FA-Token nicht verfügbar ist, und sind nicht auf die Unterstützung des IT-Supports angewiesen.

Welche IT-Sicherheitstipps können TU Graz-Mitarbeitende einfach umsetzen?

- **Halten Sie Ihr Betriebssystem und Ihre Programme immer auf dem aktuellen Stand.** So erhalten Sie laufende Sicherheitsupdates, die Angreifer*innen das Leben schwerer machen.
- Stellen Sie Ihren Browser und Ihr E-Mail-Programm sicher ein, um Bedrohungen schon im Vorfeld zu unterbinden. Hilfreiche Infos dazu finden Sie unter: ▸ **security.tugraz.at**
- Besuchen Sie den Kurs **„Cybersecurity – Phishing und andere Sicherheitsbedrohungen“** der Internen Weiterbildung und werden Sie noch sicherer im Umgang mit E-Mail, Internet und Co.

Cybersecurity an der TU Graz

Die TU Graz ist tagtäglich IT-Angriffsversuchen ausgesetzt, die allermeisten davon laufen jedoch dank der Sicherheitsvorkehrungen unserer Universität von Anfang an ins Leere. Angesichts der Menge an Angriffen und der gestiegenen Sicherheitsanforderungen ist es wichtig, den Schutz stets weiter zu verbessern, so hat die TU Graz erst kürzlich ihre Firewall optimiert. Zudem gilt es, potenzielle Sicherheitslücken zu orten und zu beheben – beispielsweise ist es in Sonderfällen notwendig, an einem Institut auch veraltete Betriebssysteme einzusetzen, um in der Forschung benötigte Programme weiterhin ausführen zu können. In solchen Fällen ist es wichtig, die betreffenden Geräte vom TU Graz-Netzwerk zu trennen, sodass sie nicht zu einem potenziellen Einfallstor für Angriffe werden – bitte wenden Sie sich dazu an den Zentralen Informatikdienst.

TU Graz *people*

Nr. 84 2023-02

Magazin für TU Graz-Mitarbeitende und Interessierte