Tipps für die Cybersicherheit

Die Anzahl von Cyberangriffen und deren Komplexität nehmen allgemein zu. Deshalb ist es wichtiger denn je, Online-Kriminellen stets einen Schritt voraus zu sein. Die folgenden Tipps könnten für den Schutz Ihrer Daten wichtig sein, selbst in Krisenzeiten:

1 – Seien Sie auf der Hut vor Phishing-E-Mails und Scheinanrufen

- Achten Sie auf ungewöhnliche oder dringende Anforderungen, die Sie per E-Mail, Telefon oder SMS (Textnachricht) erhalten.
- Prüfen Sie die Echtheit einer Anfrage, bevor Sie mit Personen, die Sie nicht kennen, Informationen teilen. Klicken Sie niemals auf Links oder laden Sie Anhänge herunter, bei denen Sie Zweifel haben.
- Hüten Sie sich vor betrügerischen Anrufen. Geben Sie am Telefon niemals Informationen preis, falls Sie an der Echtheit des Anrufers zweifeln.

2 – Bleiben Sie online auf der sicheren Seite

- Besuchen Sie nur vertrauenswürdige Webseiten und speichern Sie diese als Favoriten. Eine sichere Webseite beginnt mit "https://". Daten, die Sie mit einer solchen Website austauschen, können nicht abgefangen oder geändert werden.
- Nutzen Sie, wenn immer möglich, eine Multi-Faktor-Authentifizierung. Andernfalls arbeiten Sie mit einzigartigen, starken Passwörtern und verwalten Sie diese mit einem Passwort-Manager.
- Informieren Sie sich zum Geschehen in der Welt nur über bekannte, seriöse Quellen und spenden Sie nur über offizielle Kanäle.

3 – Hüten Sie sich vor öffentlichen Wifi-Hotspots und schädlichen Downloads

- Seien Sie vorsichtig bei öffentlichen Wifi-Hotspots. Vermeiden Sie es, diese für das E-Banking, zum Senden von E-Mails oder für Sozialen Medien zu nutzen. Hacker könnten sich auf diesem Wege Zugriff auf Ihre Informationen verschaffen.
- Laden Sie Software nur von vertrauenswürdigen App-Stores herunter und halten Sie diese auf dem neuesten Stand.

4 – Teilen Sie Informationen mit Vorsicht

- Achten Sie darauf, was Sie auf Sozialen Medien teilen und dort als "gefällt mir" markieren.
- Vermeiden Sie es, persönliche Informationen wie Geburtsdatum, Wohnanschrift, Kontaktangaben, Urlaubszeiten und andere Angaben, die von Kriminellen ausgenutzt werden könnten, zu posten (oder in Ihren öffentlichen Profilen anzugeben).
- Fügen Sie Ihrem Netzwerk nur Ihnen bekannte Personen hinzu und schränken Sie über Datenschutzkontrollen ein, wer was sehen kann.

5 – Innehalten. Nachdenken. Handeln.

- Halten Sie inne, wenn etwas nicht richtig erscheint.
- Überdenken Sie die Risiken.
- Seien Sie vorsichtig bei all Ihren digitalen Aktivitäten.

Denken Sie daran: UBS fordert ihre Kunden niemals per Anruf, E-Mail oder SMS zum Login oder zur Angabe ihrer Zugangsdaten auf. Wir versenden keine E-Mails mit Links zu Anmeldeseiten wie E-Banking-Vertragsnummer oder PIN.