Digitale Sicherheit.
Für Mensch & Maschine.

AWARE7
full service awareness agency

Top 10 IT-Security Tipps

Die digitale Identität muss aktiv geschützt werden. Sie können einen erheblichen Beitrag dazu leisten, nicht Opfer von z.B. Identitätsdiebstahl zu werden. Befolgen Sie folgende Tipps und setzen Sie die Handlungsempfehlungen konsequent um - dann haben es Cyberkriminelle allzu schwer Ihre Accounts zu knacken. Wir wünschen Ihnen bei der Umsetzung viel Erfolg!

1. Starke und verschiedene Passwörter verwenden

Ein Passsatz, eine Gedankenstütze oder ein (Off- oder Online) Passwortmanager können dabei helfen, für jede Website und jeden Dienst unterschiedliche und starke Passwörter zu erstellen und zu verwalten. Laden Sie jetzt Ihren persönlichen Kryptzonizer herunter (https://passwort-ausdenken.de). So können einfache Wörter in ein schwer zu knackendes Passwort überführt werden.

2. Fremdzugriffe erschweren und Zwei-Faktor-Authentifizierung verwenden

Geräte sollten, sobald der Platz verlassen wird, gesperrt werden - auch dann, wenn es nur einen Augenblick ist! Wenn es die Internetseite anbietet, sollten Sie auch die Zwei-Faktor-Authentifizierung aktivieren und keinen Gebrauch von der Funktion “angemeldet bleiben” machen. Unter https://zweiterfaktor.de können Sie nachschauen, welcher Anbieter ihnen welche Möglichkeiten anbietet, sich zusätzlich zu authentifizieren.

3. Updates und Patches installieren

Um bekannte Sicherheitslücken zu schließen, sollte Software stets auf dem aktuellen Stand gehalten werden. Aktuelle Software ist mit der beste Schutz vor Schadsoftware. Eine frühzeitige Installation von Updates und Patches schützt Sie. Den Windows Defender sollten Sie auf einem Windows Betriebssystem stets aktivieren. Dieser schützt ebenfalls vor Schadsoftware.

4. Seien Sie skeptisch bei dringendem Handlungsbedarf

Angebote, Gewinnspiele oder Warnungen die auf den ersten Blick seriös erscheinen und eine umgehende Handlung erfordern, sollten genau betrachtet werden. Häufig stecken Phishingangriffe dahinter und zielen darauf ab Daten zu sammeln.

5. Bewusst mit persönlichen Daten umgehen

Geteilte Informationen lassen sich nur schwer bis gar nicht aus dem Internet entfernen. Viele Informationen sind bereits gestohlen worden. Eine wichtige Information ist, ob Sie bereits Opfer von Datendiebstahl geworden sind. Das können Sie selbstständig überprüfen. Besuchen Sie dafür die Internetseite https://haveibeenpwned.com. Alternativ dazu gibt es ein deutschsprachiges Angebot vom Hasso-Plattner-Institut aus Potsdam https://sec.hpi.de/ilc/

6. Ungesicherte Kommunikation vermeiden

Beim Besuch einer Internetseite sollte darauf geachtet werden, dass die Seite Informationen verschlüsselt empfängt. Ein HTTPS vor der Internetadresse lässt dies erkennen. Ihre Daten werden zum Betreiber der Internetseite verschlüsselt übertragen. Aber seien Sie aufmerksam - denn es bedeutet nicht, dass die Seite auch seriös ist. Fakeshops bieten auch eine verschlüsselte Verbindung an.

7. Vorsicht bei öffentlichen WLAN-Netzen

In öffentlichen, ungesicherten WLAN-Netzen sollten keine personenbezogenen Daten übertragen werden. Angreifer können die Verschlüsselung verhindern und Kommunikation mitlesen und manipulieren. Warnhinweise sollten nicht ignoriert werden.

8. Regelmäßige Backups anlegen

Wichtige Daten und Unterlagen sollten immer auf mindestens zwei getrennten Datenträgern gespeichert sein. Diese Maßnahme schützt gegen Vor- und Ausfälle der Daten. Fällt ein Datenträger aus, haben Sie noch eine Reserve. Bilder, Erinnerungen und wichtige Arbeitsdokumente sind dann nicht verloren und können wiederhergestellt werden.

9. Accountpflege betreiben

So viele Accounts wie nötig - so wenige wie möglich. Wird ein Account nicht mehr benötigt, sollte er gelöscht werden. Das ist jedoch nicht immer einfach. Damit Sie vor der Anmeldung erfahren, mit welchem Aufwand Sie bei der Abmeldung zu rechnen haben, werfen Sie vorher einen Blick auf https://cyberpflege.de.

10. Privatsphäreeinstellungen regelmäßig überprüfen

Datenschutzeinstellungen von Software und Diensten sollten regelmäßig überprüft und kontrolliert werden - besonders nach der Durchführung von Updates. Eine Überarbeitung und Zusammenführung von Einstellungen hat konkrete Auswirkungen auf die Privatsphäreeinstellungen.