SCHUTZ VOR CYBERKRIMINALITÄT:

Stand: 2021

PASSWÖRTER UND SICHERHEIT?

VIELE MENSCHEN ACHTEN AUF IHRE PERSÖNLICHEN DATEN UND GEBEN DIESE ZU RECHT NICHT AN DRITTE WEITER.

Die Realität im Umgang mit persönlichen Daten sieht in unserem Alltag jedoch sehr bedenklich aus. Zum einen werden dieselben Passwörter aus dem Privatbereich ebenso in der Firma verwendet, wo man zurzeit angestellt ist und zum anderen werden die Passwörter nicht notiert, da sie einfach gehalten werden und gut merkbar sind.

Es ist vorab zu erwähnen das sie als Benutzer jeglicher Passwort geschützten Plattformen, die eigene Verantwortung tragen und die Konsequenzen aus den daraus entstehenden Schäden, wie z.B. Datenverlust selbst tragen müssen.

Die folgenden Punkte sollen Ihnen aufzeigen, wie sie sich im Internet besser schützen können.

1. E-MAIL VON UNBEKANNTER HERKUNFT

Wenn sie eine E-Mail erhalten und sie den Absender nicht kennen, sollten sie beim öffnen der Mail vorsichtig sein. Es könnte sich dabei um eine Phishing Mail handeln. Phishing Mails werden immer professioneller gestaltet und daher wird es auch immer schwerer diese zu erkennen.

Als erste Regel gilt:
Keine Ihnen bekannte Quelle, sei es Ihre Bank, Kreditkarten Institute oder ähnliche Organisationen bei denen Sie Passwort geschützt angemeldet sind, wird Sie nach Ihren Zugangsdaten per Mail anfragen.

Als zweite Regel gilt:
Geben Sie niemals Ihre Persönlichen Daten aus der Hand, weder per Mail noch auf einem Blatt Papier an Drittpersonen. Ihre Daten sind strengvertraulich und dürfen nicht in falsche Hände geraten.

Als dritte Regel gilt:
Nutzen Sie auf all ihren Geräten welche sie für den Zugang ins Internet verwenden eine Viren Software, damit Sie vorbeugend gegen Cyberkriminalität geschützt sind.

2. PASSWORT REGELN UND IHRE SICHERHEIT

Achten Sie bei der vergabe eines Passwortes darauf, dass Sie nicht Ihren Namen, Geburtsdatum oder ähnliches verwenden. Solche Passwörter sind sehr leicht herauszufinden.

Als erste Regle gilt:
Notieren Sie Ihre Passwörter in ein dafür vorgesehenes Notizbuch, um es später nicht zu verlieren.

Als zweite Regel gilt:
Benutzen Sie niemals dieselben Passwörter aus Ihrem Privat- und Geschäftlichen Bereich.

Als dritte Regel gilt:
Verwenden Sie für verschiedene Plattformen auch verschiedene Passwörter, es empfiehlt sich nicht dieselben Passwörter für verschiedene Plattformen zu benutzen. Auch sollten Sie die Passwörter auf den verwendeten Plattformen ab und zu wechseln.

Als vierte Regel gilt:
Machen Sie es der Cyberkriminalität nicht leicht und generieren Sie Passwörter welche schwer bis sehr schwer herauszufinden sind.

Als Beispiel: Nehmen Sie sich kurz Zeit und erarbeiten Sie eine Passwortstruktur für sich. Diese kann z.B. wie folgt aussehen:

z.B.:
Google Login
Benutzername: Hans Muster
Passwort: 674_Ha_476_Mu

Durch die Sonderzeichen, Gross- und Kleinbuchstaben sowie die Länge des Passwortes, ist es sehr schwer solch eine Passwort Struktur herauszufinden.

Es gibt unendlich viele Strukturen, welche Sie für sich generieren können. Entscheiden Sie sich jedoch nicht gleich für unser Beispiel, damit es dann nicht von Millionen von Menschen genutzt wird 😉

2 SCHRITTE AUTHENTIFIRZIERUNG

Durch die Aktivierung der 2 Schritte Authentifizierung sichern Sie sich noch zusätzlich ab und schützen Ihre Daten vor unerwünschtem Missbrauch.

Achten Sie auf einen solchen Hinweis auf den Plattformen welche Sie benutzen und aktivieren Sie die 2 Schritte Authentifizierung.

Fazit:
Nur wenn wir uns alle an diese und weitere von unseren Internet Anbietern empfohlenen Regeln halten, werden wir unseren Beitrag dazu leisten uns sicherer im Internet aufhalten zu können.