**Phishing-Attacken: So schützen Sie sich vor Hackern**

Betrüger nutzen derzeit das Vertrauen von Bankkunden aus, um Zugangsdaten, also Benutzername und Passwort, zu deren Konten zu erhalten. Rund 80% der Vorfälle werden durch Fehlverhalten von Nutzern, aufgrund von Unachtsamkeit, ausgelöst.

**Was ist Phishing?**

Phishing zählt zu den gängigsten Cyberattacken und zielt auf persönliche, sensible Daten ab. Mithilfe gefälschter Nachrichten und Websites, die in Layout und Texten oft kaum von den Echten zu unterscheiden sind, werden die Opfer aufgefordert ihre Daten an die Betrüger freizugeben.

Dabei ist vor allem **Smishing, Phishing-Attacken per SMS**, auf dem Vormarsch. Bei der Nutzung des Smartphones, sind Benutzer weniger achtsam und gehen davon aus, dass Kurznachrichten fälschungssicherer sind als E-Mails. Dadurch werden diese Angriffe zu einem immensen Sicherheitsrisiko.

**Wie gefährlich ist Phishing?**

Phishing-Attacken betreffen sowohl Privatpersonen als auch Unternehmen. Durch den Diebstahl von Zugangsdaten, vor allem von Bankdaten haben Hacker die Möglichkeit, Transaktionen durchzuführen. Dadurch können sich Hacker sowohl bei Privatpersonen als auch bei Unternehmen hohe Geldbeträge ergaunern. Attacken auf Unternehmen können zudem enorme volkswirtschaftliche Schäden mit sich bringen, da Summen in Millionenhöhe betroffen sein können.

**Wie können Phishing-Attacken erkannt werden?**

Nachrichten, welche von Betrügern stammen weisen häufig bestimmte Merkmale auf.

Eine Auswahl dieser Merkmale sind folgende haben wir für Sie zusammengefasst:

* Beinhalten Rechtschreib- oder Grammatikfehler
* Fordern auf zum Handeln
* Signalisieren eine Dringlichkeit
* Persönliche Anrede fehlt
* Angepasste Links in der Nachricht (durch rechtsklick erscheint die verborgene Adresse)
* Zugangsdaten und Kartennummern werden erfragt
* Umlaute fehlen
* Enthalten kyrillische Zeichen
* usw.

**Wie können Sie sich schützen?**
Neben der Fähigkeit, Phishing-Attacken zu erkennen, darf ein umfangreicher Schutz natürlich nicht fehlen.

Mit diesen 8 Tipps können Sie sich schützen:

* Installieren Sie Antivirenprogramme.
* Kontrollieren Sie die E-Mail-Adresse des Absenders der Nachrichten.
* Geben Sie Ihre persönlichen und sensiblen Daten nie an Unbekannte weiter.
Kontrollieren Sie zuerst das Impressum der offiziellen Webseite und rufen Sie gegebenenfalls den Absender über diese Telefonnummer an. Nicht die Telefonnummer der Nachricht verwenden, sondern die Nummer der offiziellen Webseite.
* Öffnen Sie niemals Anhänge von unbekannten Absendern. Besonders anfällig sind jene Dateien, welche auf „.exe“, „.msi“ und „.scr“ enden.
* Nutzen Sie verschiedene Zugangsdaten für unterschiedliche Accounts. Dadurch können Angriffe auf mehrere Accounts vermieden werden.
* Greifen Sie auf Multi-Faktor-Authentifizierung zurück. Dadurch reichen Benutzername und Passwort für das Hacken eines Accounts nicht mehr aus.
* Periodische Updates und Aktualisierungen der Systeme können beim Schutz vor Hackern helfen.
* Führen Sie regelmäßig Mitarbeiter Sensibilisierungen, sogenannte IT-Awareness Trainings, durch.

Vom Antivirusprogramm über Schwachstellenanalysen und Multi-Faktor-Authentifizierung, sowie Awareness Trainings: Das IT-Unternehmen KONVERTO bietet IT-Sicherheit in allen Belangen und hilft Ihnen dabei, eine für Sie passende Security-Strategie zu erarbeiten.