Advent, Advent...

...das Postfach brennt!

E-Mails mit gefälschtem Inhalt und Absender, mit denen Angreifende versuchen uns Geld oder Daten zu entlocken, werden als **Phishing-E-Mails** bezeichnet. Diese gefälschten E-Mails sind mittlerweile weitestgehend fehlerfrei, kaum von echten E-Mails zu unterscheiden und mischen sich unbemerkt unter die übliche E-Mail-Flut zum Jahresende. Im Eifer des Gefechts hat man schnell einen infektiösen Link oder Anhang geöffnet. Ein unbedachter Klick und die Schad-software landet auf Ihrer Festplatte.

Halten Sie gerade in stressigen Zeiten einen kurzen Moment inne und stellen Sie sich folgende Fragen:

- Kenne ich die absendende Person?
- Passt der Inhalt zur absendenden Person?
- Stimmen Absendername und E-Mail-Adresse überein?
- Habe ich den Anhang oder Link erwartet?
- Enthält die E-Mail Anweisungen, vermittelt sie dringenden Handlungsbedarf oder wird mit negativen Konsequenzen gedroht?
- Mit Künstlicher Intelligenz (KI) generierte E-Mails sind von echten E-Mails kaum zu unterscheiden. Sie sind fehlerfrei und enthalten oft eine persönliche Anrede.

Goldene Regel

Folgen Sie niemals einer Aufforderung, wenn es um die Eingabe persönlicher Informationen oder Zugangsdaten geht.
Rufen Sie stattdessen das zugehörige Benutzerkonto (bspw. Ihren Online-banking-Account) über den Ihnen bekannten Link auf und prüfen Sie, ob tatsächlich Handlungsbedarf besteht.

Öffnen Sie beim geringsten Zweifel weder Links noch Anhänge. Kontaktieren Sie umgehend Ihre IT-Abteilung und folgen Sie deren Anweisungen.

Mit diesen Tipps bleiben Ihr Postfach und Ihre Festplatte frei von Schadsoftware. Damit steht einem besinnlichen Weihnachtsfest nichts mehr im Weg.

CSBW
CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

Mit uns.
Mit Ihnen.
Mit Sicherheit.