Fallen Sie nicht auf den

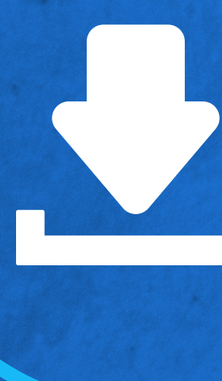
PHISHING-Köder herein

Seien Sie misstrauisch gegenüber...

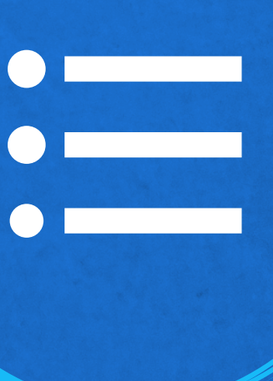
Hyperlinks zu gefälschten Websites

Inoffizielle "Von"-Adressen

"Dringende" Anfragen oder Drohungen



E-Mails mit Anhängen



Anfragen für sensible Informationen

"Sehr geehrter Benutzer"

Generische Betreffzeilen und Intro-Nachrichten

Versenden Sie sensible Daten per E-Mail?

Stellen Sie sicher, dass Sie nicht den falschen Empfänger eingegeben haben

To: XXXX
Cc: XXXX
Bcc: XXXX

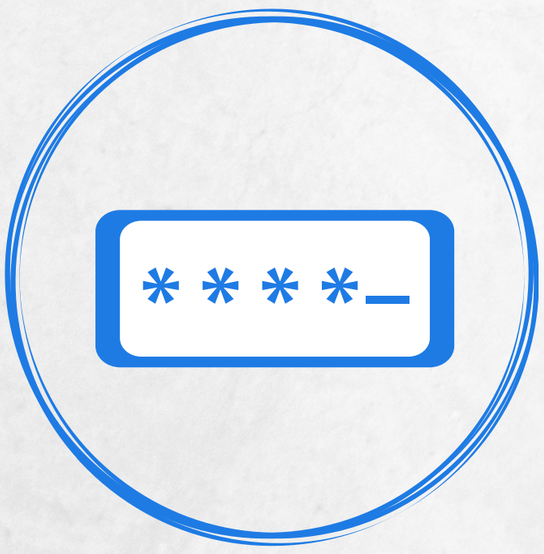
Wie stark ist Ihr Passwort?

Schwache Passwörter sind leicht zu knacken.
Halten Sie die Dinge sicher, indem Sie sicherstellen,
dass Sie...

Halten Sie es lang und kompliziert

Groß- und Kleinbuchstaben verwenden

Vermeiden Sie erratbare Informationen (z. B. D.O.B.)



Implementierung einer Zwei-Faktor-Authentifizierung

Ändern Sie Ihr Passwort regelmäßig

Geben Sie niemals Ihr Passwort weiter

Vermeiden Sie es, eine "leichte Beute" für Cyber-Kriminelle zu sein. Aktivieren Sie...

Zwei-Faktor-Authentifizierung

Sensible Daten per E-Mail versenden?

To: XXXX

Cc: XXXX

Bcc: XXXX

Überprüfen Sie immer, ob Sie den richtigen Empfänger eingegeben haben.

Unterwegs?

Bitte gehen Sie vorsichtig mit physischen Daten um, wenn Sie sie außer Haus bringen.

Verlassen Sie Ihren Schreibtisch?

Sichern Sie Ihre Daten, indem Sie Ihren Computer und Ihre Geräte sperren, wenn sie **nicht benutzt werden**.