

# 5 Cyber Regeln für das digitale Leben

Indem Sie unsere 5 Cyber Regeln befolgen, können Sie im Alltag sicherer unterwegs sein.



1

## Schützen Sie Ihre Daten und Geräte



- **Halten Sie Ihre Software up-to-date**, auf allen Geräten.
- **Aktualisieren Sie Ihre Software** über vertrauenswürdige Quellen

- **Googeln Sie sich**, um herauszufinden, welche Informationen über Sie öffentlich verfügbar sind.
- Überprüfen Sie Ihre **Privatsphäre-Einstellungen** auf Social Media.



## 2 Seien Sie online und in der Öffentlichkeit diskret

## 3 Denken Sie nach, bevor Sie klicken und antworten



- **Seien Sie vorsichtig** bei verdächtigen E-Mails und klicken Sie nicht auf verdächtige Links oder Anhänge.
- **Wenn Sie unsicher sind**, kontaktieren Sie den/die Absender/in über Ihnen bekannte oder öffentlich zugängliche Kontaktdaten und nicht über die Kontaktdaten der verdächtigen E-Mail.

- **Verwenden Sie Passwortphrasen** (3 oder mehr Wörter) als Passwort, diese sind sicher und leichter zu merken.
- Wenn möglich, verwenden Sie die „**Zwei-Faktor-Authentifizierung**“.



## 4 Schützen Sie Ihre Passwörter

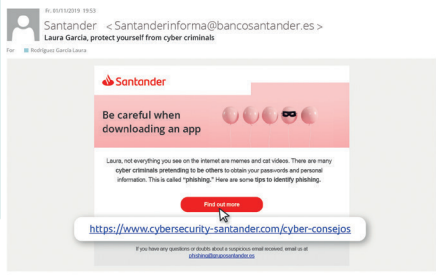
## 5 Wenn Ihnen etwas verdächtig vorkommt, melden Sie es



- **Wenn Sie einen Anruf oder eine Nachricht von Santander erhalten**, die Ihnen verdächtig vorkommt, melden Sie es an [infoservice@santanderconsumer.at](mailto:infoservice@santanderconsumer.at) oder kontaktieren Sie uns telefonisch unter 050203 1800.

Seien Sie online sicher und teilen Sie diese Tipps mit Ihren Freunden und Bekannten.

Jeder Klick zählt!



## Phishing

Ein betrügerischer Versuch, persönliche Informationen mit Hilfe von Social-Engineering-Techniken zu erlangen oder sich in einer elektronischen Kommunikation als vertrauenswürdige Unternehmen auszugeben.



## Malware

Eine Art von Software, die versucht, ein Gerät zu beeinflussen und/oder zu beschädigen, indem sie ohne das Wissen des Benutzers darauf zugreift.

## Virus

Ein Computervirus ist ein Computerprogramm, das dazu dient, die Funktion eines Geräts ohne die Erlaubnis oder das Wissen des Benutzers zu verändern.



## MFA

Multi-Faktor-Authentifizierung (MFA) ist eine besonders sichere Art der Anmeldung, bei der nicht nur ein Passwort abgefragt wird, sondern auch eine oder mehrere zusätzliche Verifizierungen, wie ein Bestätigungscode oder Ihr Fingerabdruck.



## Sichere Website

HTTPS (Hypertext Transfer Protocol Secure) ist ein Kommunikationsprotokoll, das die Daten der Benutzer bei der Übertragung zwischen ihren Computern und einer Website schützt. Es bietet höhere Sicherheit als das HTTP-System.

## Sicherungskopie

Eine Kopie von Daten, die auf einem anderen Gerät erstellt wird. Ziel ist es, die Daten wiederherstellen zu können, falls sie verloren gehen.



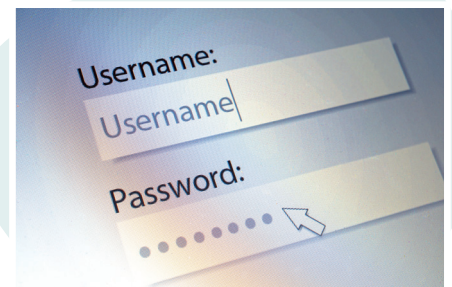
## Social Engineering

Die Praxis, vertrauliche Informationen durch Manipulation und Nachahmung der Identität legitimer Benutzer zu erlangen.



## Passphrase

Ein Passwort, das aus drei oder mehr Wörtern (wie ein Satz) besteht und die Sicherheit erhöht, da es schwieriger zu knacken ist als ein Passwort mit nur einem Wort.



## Datenschutz-Einstellungen

Eine Reihe von Einstellungen, die Nutzer verwalten können, um zu kontrollieren, welche Informationen sie an wen weitergeben.



## Verschlüsselung

Eine verschlüsselte Nachricht ist durch einen Algorithmus geschützt und nur Personen mit Berechtigung können darauf zugreifen.

