Sicher unterwegs im Internet

Bleiben Sie wachsam und schützen Sie sich und Ihre Daten!

# Phishing

Betrüger verwenden gefälschte E-Mails oder Webseiten verwenden, um sensible Informationen wie Passwörter oder Kreditkartendaten zu stehlen.

* **E-Mails und Links prüfen**: Öffnen Sie keine Links oder Anhänge in E-Mails von unbekannten Absendern.
* **Absenderadresse überprüfen**: Achten Sie auf ungewöhnliche Absenderadressen oder Rechtschreibfehler.
* **Keine persönlichen Daten preisgeben**: Geben Sie niemals Passwörter oder persönliche Informationen preis.

# Fiscal inspetor pessoas dinheiro emoji - Ícones Avatar e EmoticonsCEO-Betrug

Kriminelle geben sich als hochrangige Führungskräfte ausgeben, um Mitarbeiter zur Überweisung von Geld oder zur Preisgabe vertraulicher Informationen zu verleiten.

* **Anfragen verifizieren**: Überprüfen Sie ungewöhnliche Anfragen von Vorgesetzten telefonisch oder persönlich.
* **Auffällige E-Mails melden**: Informieren Sie die IT-Abteilung über verdächtige E-Mails.

# Viren

Schadsoftware, die sich selbst repliziert und Computersysteme infiziert, um Daten zu stehlen, zu beschädigen oder zu löschen.

* **Antivirensoftware nutzen**: Installieren und aktualisieren Sie regelmässig eine zuverlässige Antivirensoftware.
* **Downloads vermeiden**: Laden Sie keine Dateien von unbekannten oder unsicheren Quellen herunter.

# Gefälschte Drohmails / Fake Sextortion

E-Mails, die vorgeben, von Strafverfolgungsbehörden oder anderen offiziellen Stellen zu stammen, um den Empfänger zur Zahlung von Geld zu erpressen.

Fake Sextortion: Eine Betrugsmasche, bei der Kriminelle behaupten, kompromittierende Fotos oder Videos des Opfers zu besitzen und Geld verlangen, um diese nicht zu veröffentlichen.

* **Nicht reagieren**: Antworten Sie nicht auf Drohmails und geben Sie keine Zahlungen frei.
* **IT-Abteilung informieren**: Melden Sie solche E-Mails sofort der IT-Abteilung.

# Ransomware Vector Icon Design 21315527 Vector Art at VecteezyRansomware

Schadsoftware, die Daten auf einem infizierten System verschlüsselt und ein Lösegeld fordert, um den Zugriff auf die Daten wiederherzustellen.

* **Regelmässige Backups**: Erstellen Sie regelmässig Backups wichtiger Daten und speichern Sie diese offline.
* **Software aktuell halten**: Halten Sie Betriebssysteme und Anwendungen stets auf dem neuesten Stand.

# Premium Vector | Hacker icon vectorSocial Media Hacking

Unbefugter Zugriff auf Social-Media-Konten, oft um persönliche Informationen zu stehlen oder betrügerische Aktivitäten durchzuführen.

* **Starke Passwörter verwenden**: Nutzen Sie komplexe Passwörter und ändern Sie diese regelmässig.
* **Privatsphäre-Einstellungen prüfen**: Überprüfen und beschränken Sie die Sichtbarkeit Ihrer Social Media-Profile.

# Ein Bild, das Clipart, Grafiken, Silhouette, Cartoon enthält.  KI-generierte Inhalte können fehlerhaft sein.Fake Support

Betrüger, die sich als technische Supportmitarbeiter ausgeben, um Zugang zu Computern oder sensiblen Informationen zu erhalten.

* **Unaufgeforderte Anrufe ignorieren**: Reagieren Sie nicht auf unaufgeforderte Anrufe von angeblichen Support-Diensten.
* **Offizielle Kanäle nutzen**: Kontaktieren Sie den Support immer über offizielle Kanäle.

# Social engineer icon Royalty Free Vector ImageSocial Engineering

Manipulationstechniken, die darauf abzielen, Menschen zur Preisgabe vertraulicher Informationen zu verleiten, oft durch das Vortäuschen einer vertrauenswürdigen Identität.

* **Misstrauisch sein**: Seien Sie vorsichtig bei Anfragen nach vertraulichen Informationen, auch wenn sie von bekannten Personen zu kommen scheinen.
* **Schulungen besuchen**: Nehmen Sie an Schulungen zum Thema Social Engineering teil.

# Ein Bild, das Screenshot, Grafiken, Farbigkeit, Grafikdesign enthält.  KI-generierte Inhalte können fehlerhaft sein.Quishing

Eine spezielle Form des Phishings, bei der QR-Codes verwendet werden, um Benutzer auf gefälschte Webseiten zu leiten und ihre Daten zu stehlen.

* **QR-Codes prüfen**: Scannen Sie keine QR-Codes aus unbekannten Quellen.
* **URL überprüfen**: Achten Sie darauf, dass die URL nach dem Scannen des QR-Codes vertrauenswürdig ist.

Bei Fragen oder Unsicherheiten hilft Ihnen die IT-Abteilung weiter.