EINIGE TIPPS, UM SICHER IM INTERNET ZU SURFEN

Eine vertrauenswürdige Sicherheitslösung

- Wählen Sie komplette Sicherheits-Suiten anstatt einfacher Antivirus-Programme (vor allem, wenn sie kostenlos sind), da sie mehr Funktionen für Ihre Sicherheit bieten.

Speichern Sie regelmäßig Ihre Daten

- Erstellen Sie Backups in einer sicheren Cloud oder auf einer externen Festplatte, die Sie nach abgeschlossenem Backup ausstecken.

Aktualisieren Sie Ihre Geräte

- Aktivieren Sie die Optionen für automatische Aktualisierungen in den Einstellungen von Windows, macOS, Android und iOS.

Installieren Sie Ihre Apps nur über offizielle Websites oder Stores

- Nutzen Sie auf Mobiltelefonen App Store oder Google Play. Für Windows gehen Sie auf die Internetseiten der Hersteller.

Verwenden Sie ein unterschiedliches Passwort für jeden Service

- Ein Passwort-Verwalter verwaltet automatisch verschiedene und sichere Benutzerkennungen.

Aktivieren Sie die doppelte Authentifizierung, wenn dies möglich ist

- Die doppelte Authentifizierung kann per SMS oder auch über eine Mobile-App erfolgen.

Vermeiden Sie öffentliche oder unbekannte WLAN-Netzwerke

- Verwenden Sie ein VPN, um Ihren Datenverkehr zu verschlüsseln und Ihre Daten zu schützen.

Vorsicht ist bei USB-Sticks und -Datenträgern geboten.

- Bestimmte Antivirus-Programme scannen den Inhalt von USB-Datenträgern für mehr Sicherheit.

WIE KANN MAN SICH GEGEN ONLINE-BEDROHUNGEN SCHÜTZEN?

18.750 neue Viren
und Bedrohungen tauchen stündlich im Internet auf

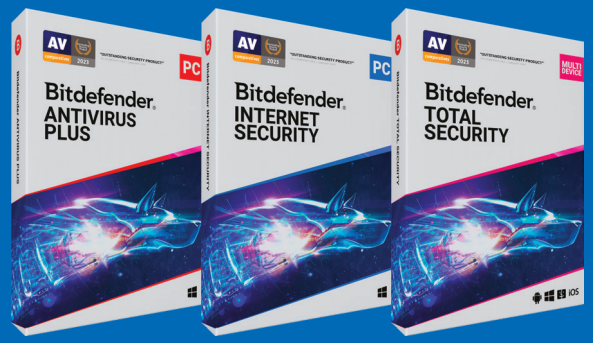
650 € Lösegeld
müssen durchschnittlich bezahlt werden, um wieder Zugriff auf die gehackten Daten zu erhalten.

2,1 Millionen neue Phishing-Webseiten
werden monatlich gefunden.

Suchen Sie eine Antivirus-Lösung?

Bitdefender

Das beste Schutzniveau am Markt



(1) Bitdefender Internet Security, Januar 2024 https://www.av-comparatives.org/tests/summary-report-2023/
(2) https://www.av-test.org/en/antivirus/home-users/

Bitdefender / FERRARI TEAM PARTNER

Bitdefender

RISIKEN IM INTERNET

ERKLÄRUNGEN & BERATUNG

WIE KANN MAN SICH SCHÜTZEN?

Trusted. Always.

FALSCHER TECHNISCHER SUPPORT

Beim Betrug mit gefälschtem technischem Support geht es darum, Ihnen Angst zu machen. Der Cyberkriminelle kontaktiert Sie per SMS, Telefon, Chat, E-Mail oder über eine Pop-up-Nachricht auf Ihrem Computer. Sie werden über ein schwerwiegendes technisches Problem und das Risiko eines Datenverlusts informiert, damit Sie eine Telefonnummer anrufen, um Hilfe zu erhalten*. Nachdem der Cyberkriminelle die Kontrolle über den PC übernommen hat, um eine Lösung des Problems vorzutäuschen und Software zu installieren oder Abonnements abzuschließen, wird er auch versuchen, Ihnen Geld zu entwenden, indem er Ihre Bankdaten abfragt.

SUPPORTBETRUG

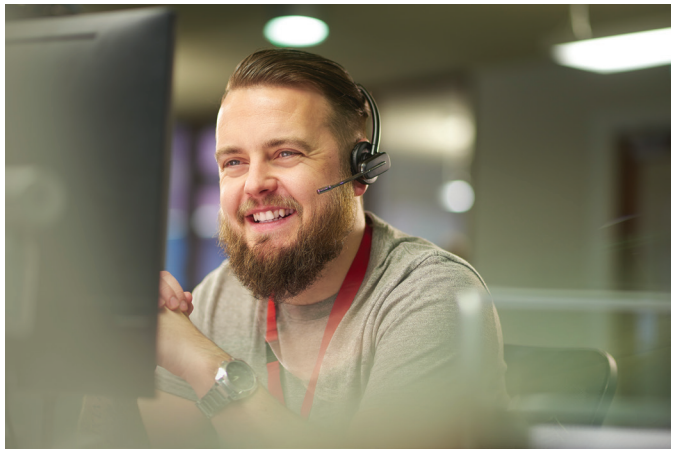
Ihr PC ist blockiert und Sie werden aufgefordert, einen technischen Support zurückzurufen? Wurden Sie Opfer eines Supportbetrugs?

ZIEL

Das Opfer wird dazu verleitet, für eine scheinbare Computerreparatur zu bezahlen und/oder kostenpflichtige Abonnements abzuschließen.

VORGEHENSWEISE

Es wird der Anschein erweckt, dass ein schwerwiegendes technisches Problem vorliegt, das die Gefahr eines Daten- oder Nutzungsverlusts der Ausrüstung mit sich bringt (durch blockierten Bildschirm, Telefon, SMS, E-Mail usw.).



TIPPS

- Reagieren Sie nicht auf Nachrichten oder Anrufe von Personen, die Ihnen nicht bekannt sind
- Beweise aufbewahren
- Ihr Gerät neu starten
- Eine Antivirus-Analyse durchführen
- Alle Passwörter ändern
- Bei Ihrer Bank Widerspruch einlegen, wenn Sie Zahlungen getätigt haben
- Klage einreichen

RANSOMWARE

Ransomware ist eine Malware, die den Zugriff auf Ihr Gerät oder Ihre Dateien blockiert, indem sie diese verschlüsselt. Der Cyberkriminelle fordert die Zahlung von Lösegeld, um wieder Zugriff zu erhalten. Ihr Gerät kann mit Ransomware infiziert werden, nachdem Sie einen Anhang geöffnet haben, auf einen schädlichen Link in einer E-Mail geklickt haben, einfach nur auf gefährlichen Webseiten surfen oder als Folge eines Eindringens in Ihr System.

RANSOMWARE

Sie können nicht mehr auf Ihre Dateien zugreifen und es wird ein Lösegeld verlangt?
Sie sind möglicherweise Opfer eines Ransomware-Angriffs!

ZIEL

Forderung eines Lösegelds, um die gesperrten Dateien wieder freizugeben.

VORGEHENSWEISE

Blockieren des Zugriffs auf Daten durch Senden einer Nachricht mit bösartigen Links oder Anhängen oder durch Eindringen in das System.

TIPPS

- PC vom Internet und lokalen Netzwerk trennen
- Kein Lösegeld zahlen
- Klage einreichen
- Lassen Sie sich von Fachkräften oder fachkundigen Bekannten helfen
- Stellen Sie die Daten aus dem Backup wieder her

PHISHING

Phishing ist ein Betrug, bei dem sich jemand als vertrauenswürdiger Dritter ausgibt, um Sie dazu zu verleiten, Ihre persönlichen Daten wie Logins, Passwörter und/oder Bankdaten preiszugeben. Es kann sich um gefälschte Nachrichten, SMS oder Telefonanrufe von Banken, sozialen Netzwerken, Telefonanbietern, Energieversorgungsunternehmen, Online-Handelsseiten, Behörden usw. handeln.

PHISHING-VERSUCHE

Sie erhalten eine unerwartete oder sogar alarmierende Nachricht oder einen Anruf von einer scheinbar offiziellen Organisation, die Sie nach persönlichen Informationen oder Bankdaten fragt. Sie sind möglicherweise Opfer eines Phishing-Angriffs!

ZIEL

Diebstahl von personenbezogenen oder beruflichen Informationen (Identität, Adressen, Konten, Passwörter, Bankdaten ...) zwecks betrügerischer Verwendung.

VORGEHENSWEISE

Lockmittel, das über eine gefälschte Nachricht, SMS, manchmal auch per Post oder Telefonanruf von Behörden, Banken, Netzbetreibern, sozialen Netzwerken, E-Commerce-Websites usw. versendet wird.

TIPPS

- Übermitteln Sie niemals sensible Daten als Antwort auf eine Nachricht oder im Rahmen eines Telefonanrufs
- Bei geringsten Zweifeln wenden Sie sich zur Bestätigung direkt an die betroffene Organisation
- Lassen Sie sofort Ihre Karte sperren (im Falle eines Bankbetrugs)
- Die offengelegten Passwörter ändern
- Klage einreichen
- Vorfälle auf speziellen Websites melden (siehe nützliche Links).