Sicherheit

E-Mail Erpressung: ALARM - I'm hacked you and stolen you information and photo

Aktuell werden viele Mailnachrichten versendet welche persönliche Daten von Menschen beinhalten, so zum Beispiel ein Passwort welches aktuell genutzt wird.

Wichtig, diese Nachricht ist kein Witz!

Die Nachricht wird meist von der eigenen Mailadresse aus gesendet, eine Prüfung der Mailnachricht hat ergeben, dass die Angreifer sich beim Mailkonto eingeloggt haben und die Mailnachricht darüber versendet haben.

Dazu konnten wir in den letzten 2 Wochen feststellen, wie Passwörter kurze Zeit nach erhalt der Mailnachricht aktiv verwendet wurden, um Zugriff auf weitere Dienste wie Spotify, Facebook oder TikTok zu erlangen. Das Vorgehen ist jeweils ähnlich, anmelden und zuerst die Rücksetz-Mailadresse anpassen.

Was muss ich tun, wenn ich ein solches Mail erhalten habe?
Das Passwort ändern, jetzt!

Das Passwort, welches im Mail ersichtlich ist, gilt ab sofort als verbrannt! Es darf nirgendwo (wirklich nirgendwo, ohne Ausnahme!) mehr verwendet werden, auch nicht in einer abgewandelten Form. Das verbrannte Passwort wird ab sofort in den grossen Passwortlisten der Welt gehandelt und kann nun relativ schnell (unter 1 Minute) geknackt werden.

Was kann ich noch tun?

- Nutze verschiedene Passwörter, ein Passwort pro Dienst.
- Schalte 2FA/MFA ein. Ja, eine mehrfache Authentifizierung kann wirklich mühsam sein, aber es erhöht den Schutz massiv.
- Nutze einen Passwortmanager, so ist es einfacher Passwörter zu verwalten. https://www.srf.ch/sendungen/kassensturz-espresso/tests/gadgets-elektronik/security-test-diese-passwortmanager-schuetzen-vor-hackern

Beispielnachricht

Sicherheit

Hey swissonline.ch,
I have to share bad news with you.
Approximately few months ago I have gained access to your devices, which you use for internet browsing.
After that, I have started tracking your internet activities.
Some time ago I hacked you and got access to your email accounts
›swissonline.ch

Obviously, I have easily hack to log in to your email.
Your password:
Dein-Passwort!

One week later, I have already installed Trojan virus to Operating Systems of all the devices that you use to access your email.
In fact, it was not really hard at all (since you were following the links from your inbox emails).
All ingenious is simple. =)

This software provides me with access to all the controllers of your devices (e.g., your microphone, video camera and keyboard).
I have downloaded all your information, data, photos, web browsing history to my servers.
I have access to all your messengers, social networks, emails, chat history and contacts list.
My virus continuously refreshes the signatures (it is driver-based), and hence remains invisible for antivirus software.
Likewise, I guess by now you understand why I have stayed undetected until this letter...
While gathering information about you, I have discovered that you are a big fan of adult websites.
You really love visiting porn websites and watching exciting videos, while enduring an enormous amount of pleasure.
Well, I have managed to record a number of your dirty scenes and montaged a few videos, which show the way you masturbate and reach orgasms.
If you have doubts, I can make a few clicks of my mouse and all your videos will be shared to your friends, colleagues and relatives.
I have also no issue at all to make them available for public access.

I guess, you really don't want that to happen, considering the specificity of the videos you like to watch, (you perfectly know what I mean) it will cause a true catastrophe for you.
Let's settle it this way:
You transfer $400 USD to me (in bitcoin equivalent according to the exchange rate at the moment of funds transfer), and once the transfer is received, I will delete all this dirty stuff right away.
After that we will forget about each other. I also promise to deactivate and delete all the harmful software from your devices. Trust me, I keep my word.
This is a fair deal and the price is quite low, considering that I have been checking out your profile and traffic for some time by now.
In case, if you don't know how to purchase and transfer the bitcoins - you can use any modern search engine.

Here is my bitcoin wallet:
bc1qy5yunj3v3045lfp7d4amg6rr2eyy36xz5265et

Was passiert weiter

Beispiel Spotify

Eine Spotify Anmeldung erfolgte kurze Zeit später, und die Mailadresse um das Passwort bei Spotify zurückzusetzen wurde geändert.
So hat der Benutzer keinen Zugriff mehr auf sein Abonnement und kann auch das Passwort nicht mehr zurücksetzen.

In diesem Fall sofort eine Mailnachricht an Spotify senden bzw. den Support kontaktieren.

Neue Anmeldung bei Spotify

Wir haben festgestellt, dass du dich auf einem neuen Gerät angemeldet hast. Wenn du das warst, musst du nichts weiter unternehmen.

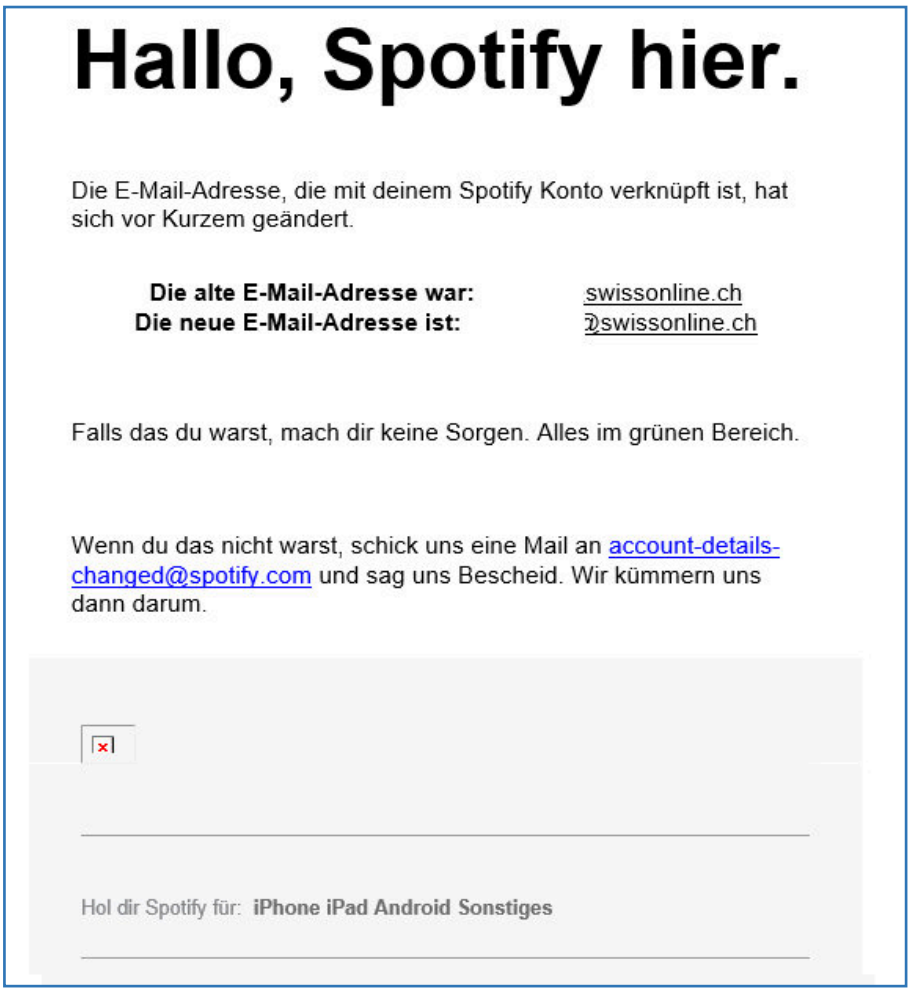
Standort **Deutschland**
Zeitpunkt **27. Juli 2023 um 11:09:18 MESZ**

Das warst nicht du?

Nimm dir ein paar Minuten Zeit, um dein Konto zu schützen.

KONTO SCHÜTZEN

Stelle sicher, dass diese E-Mail von Spotify stammt:
support.spotify.com/de/article/suspicious-email/



Hallo, Spotify hier.

Die E-Mail-Adresse, die mit deinem Spotify Konto verknüpft ist, hat sich vor Kurzem geändert.

Die alte E-Mail-Adresse war: swissonline.ch
Die neue E-Mail-Adresse ist: 2swissonline.ch

Falls das du warst, mach dir keine Sorgen. Alles im grünen Bereich.

Wenn du das nicht warst, schick uns eine Mail an account-details-changed@spotify.com und sag uns Bescheid. Wir kümmern uns dann darum.

Hol dir Spotify für: **iPhone iPad Android Sonstiges**

Sicherheit

Eindeutige ID: #1032
Verfasser: Urs Kälin
Letzte Änderung: 2023-07-28 10:30