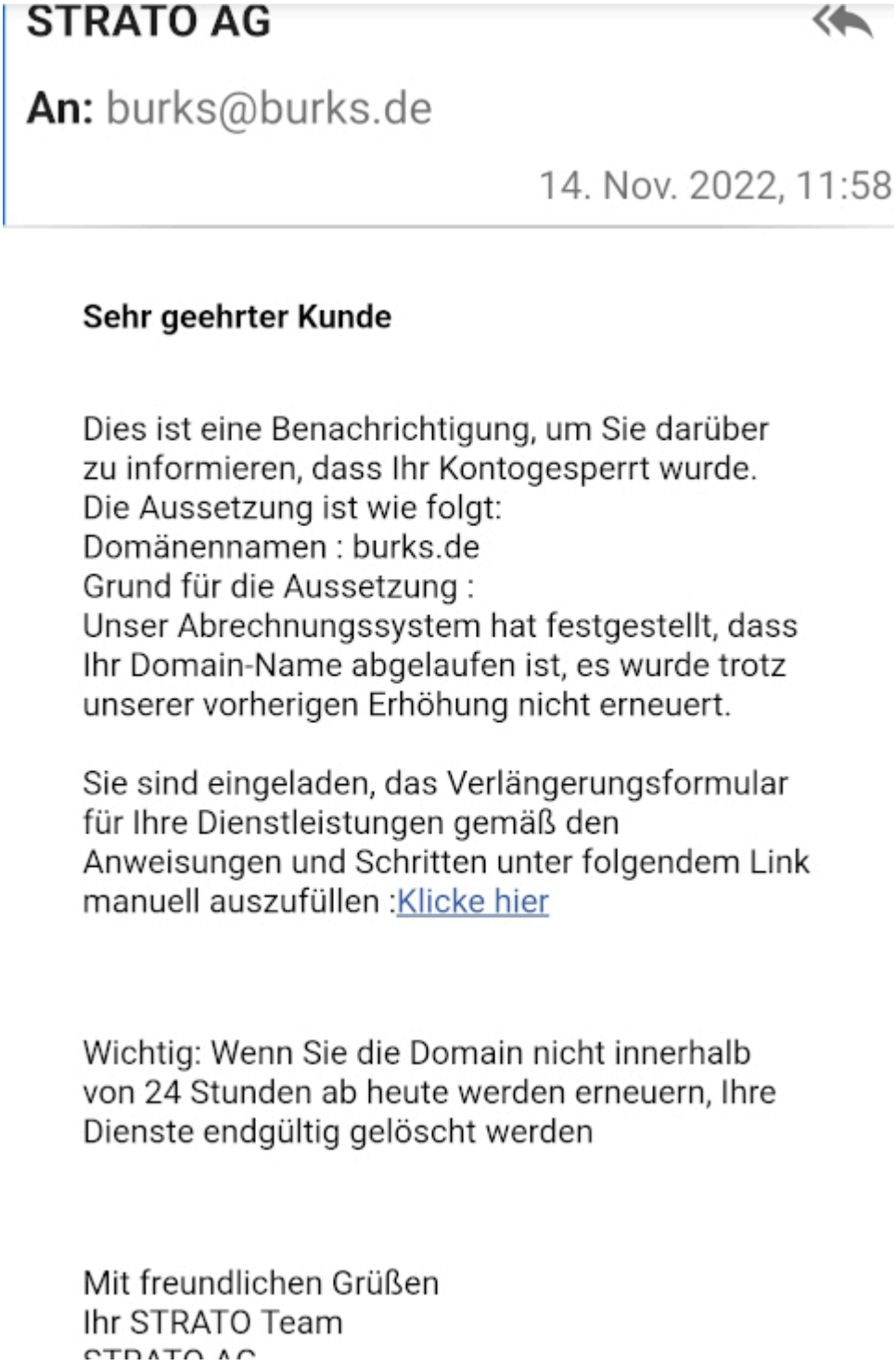
Hier Klicken oder: Доверяй, но проверяй!

Ich trage Eulen nach Athen, aber vielleicht lesen hier auch die Nachgeborenen mit, die bekanntlich nicht so IT-affin sind wie wir alten Digital Natives.

Liebe Kinder, „Hackerangiffe“ definieren wir als Blödheit der Endverbraucher, die auf alles mit der Maus oder mit dem Finger klicken, was nicht bei drei auf dem Norton Commander sitzt. Wir beschäftigen uns heute nicht mit dem Scum aus Nigeria, sondern mit den etwas klügeren Varianten. Ich werde mir nicht verkneifen können, Ratschläge zu erteilen.


STRATO AG

An: burks@burks.de

14. Nov. 2022, 11:58

Sehr geehrter Kunde

Dies ist eine Benachrichtigung, um Sie darüber zu informieren, dass Ihr Kontogesperrt wurde.
Die Aussetzung ist wie folgt:
Domänennamen : burks.de
Grund für die Aussetzung :
Unser Abrechnungssystem hat festgestellt, dass Ihr Domain-Name abgelaufen ist, es wurde trotz unserer vorherigen Erhöhung nicht erneuert.

Sie sind eingeladen, das Verlängerungsformular für Ihre Dienstleistungen gemäß den Anweisungen und Schritten unter folgendem Link manuell auszufüllen :Klicke hier

Wichtig: Wenn Sie die Domain nicht innerhalb von 24 Stunden ab heute werden erneuern, Ihre Dienste endgültig gelöscht werden

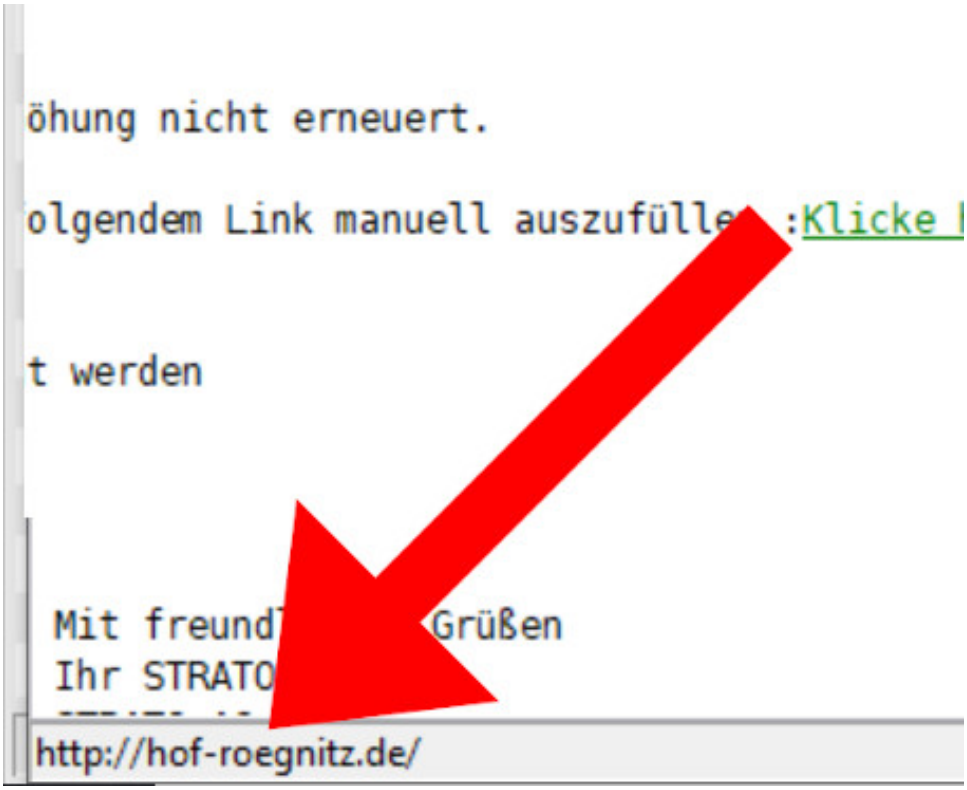
Mit freundlichen Grüßen
Ihr STRATO Team

1. Sind Postkarten wahrscheinlich?

Wichtige Dinge schickt niemand, der noch alle Tassen im Schrank hat, unverschlüsselt. Elektropost vom BKA, von Banken oder Finanzämtern usw. sind immer Spam. (Höre ich da jemanden im Hintergrund lachen?)

Frage: Wie wahrscheinlich ist es, dass Strato mir eine E-Mail schickt, obwohl ich dort gar kein Kunde bin? Oder: Wie

wahrscheinlich ist es, dass Strato einem subalternen Mitarbeiter des Rheinland-Pfalz-Kreises eine E-Mail schickt, der gar nicht weiß, ob „die Internet-Präsenz“ seiner Behörde bei Strato hängt oder nicht? Was aber, wenn ich eine E-Mail von Strato bekomme und dort einen Account habe?

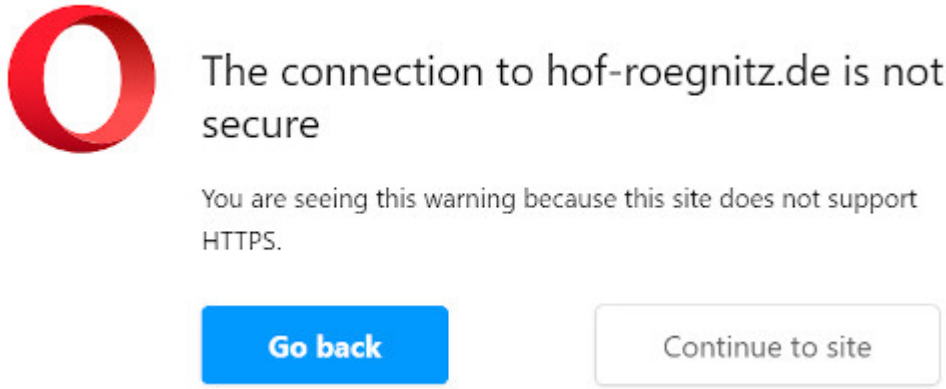


2. E-Mails nur im Textformat anzeigen lassen

~~Gibt es jemanden, der nicht weiß, wie das geht? Ich habe hier einen Screenshot aus dem letzten Jahrtausend.~~ Ich bin für nichts und niemanden repräsentativ, aber gerade jetzt sitze ich ausnahmsweise vor einem ~~tiny tits~~ schmalbrüstigen (sic) Windows-Rechner und schaue mir meine E-Mails mit Hamster und Claws Mail an. Letzteres hat die angenehme Eigenschaft, E-Mails nicht in HTML anzeigen zu können, was mich von der lästigen Pflicht befreit, in den Voreinstellungen herumfummeln zu müssen.

Trotzdem zeigt Claws Mail den Link der E-Mail nicht wirklich – der wird nur, falls man mit der Maus herumfuchtelt, unten eingeblendet. Ich werde also zum Biohof Roegnitz (hof-roegnitz.de) weitergeleitet? Seriously? In einer E-Mail von

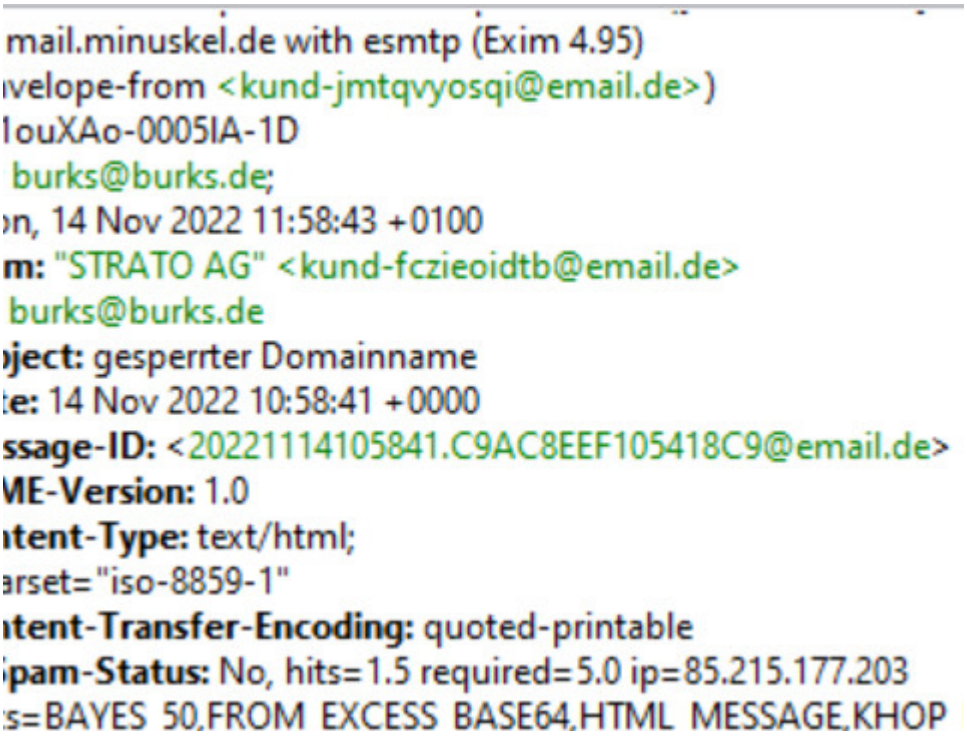
Strato?



Natürlich nicht. Aber wer schaut da schon hin ~~außer mir~~?

3. Nur [Https-Verbindungen](#) über den Cyberweg trauen

Der Browser Opera (für Windows) meckerte, als ich den vermeintlichen „Biohof“ aufrief. Ein Provider, der *keine* Website hat, die man per https aufrufen kann, sollte ohnehin als unseriös gelten. Strato aber ist [600 Millionen Euro](#) wert – da ~~sollte man nicht erwarten~~ erwartet man keine Azubis an der Servern. Hier stimmt also etwas nicht.



4. Den Header ansehen

Man kann auch in die Headerzeilen der E-Mail schauen, um Indizien zu finden, ob derjenige, der sich als Empfänger ausgibt, dort auch zu finden ist. Natürlich kann man das alles fälschen – das kann sogar ich, und der Gott der Niederlande konnte das schon 1984.

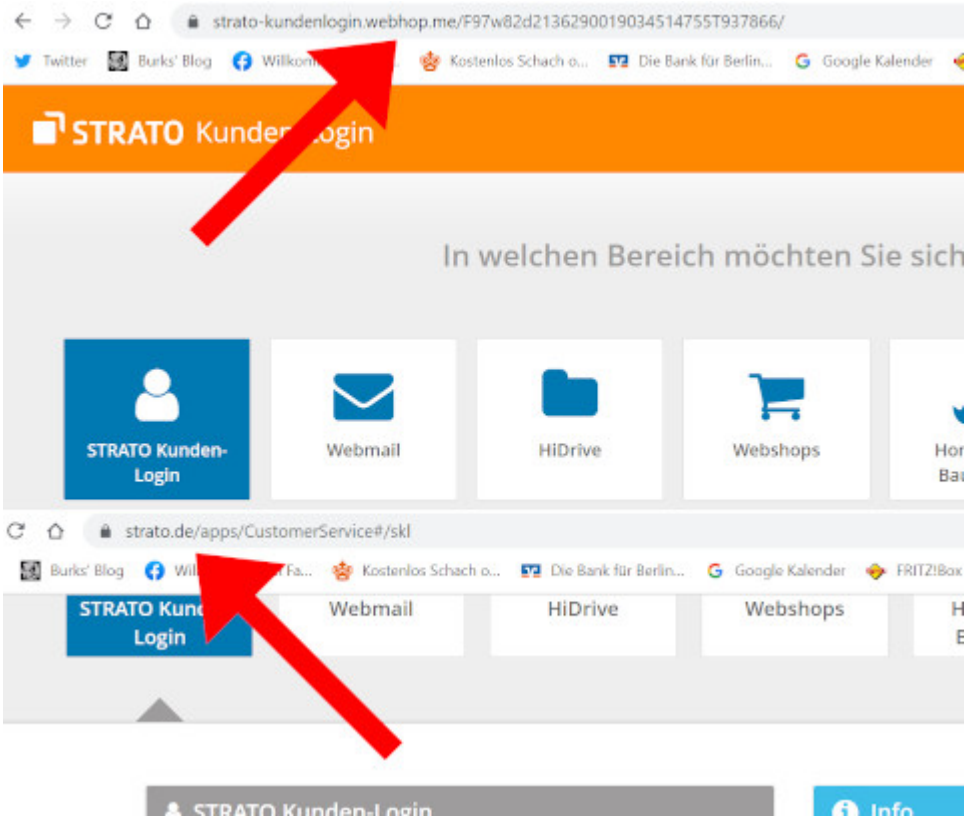
In unserem Beispiel sieht es aber eher danach aus, als schriebe jemand mit einem Web.de-Account. Der hat sich also vermutlich gar nicht die Mühe gemacht, irgendetwas zu verbergen.

Wer mit den Details der elektronischen Briefköpfe nicht vertraut ist, kann übrigens Thomas Hochstein fragen.

5. Auf die Domain oder den URL schauen

Der Link in meiner E-Mail führt für ~~DAUs~~ Unbedarfte zu einer Website, die exakt wie die bei Strato aussieht, wenn man sich einloggt. Nur die Domain ist nicht mehr eine von Strato (vgl. unten: oben die gefakte Website der Phisher, unten die Original-Website von Strato).

Die Maximen Lenins helfen nicht nur bei bewaffneten Aufständen, sondern auch bei E-Mails weiter. Ich frage mich eher, warum immer noch Leute auf die Maschen der Phishenden (sic) reinfallen? Wäre das nicht so, würden diese es nicht versuchen…


strato-kundenlogin.webhop.me/F97w82d213629001903451475ST937866/
Twitter
Burks' Blog
Kostenlos Schach o...
Die Bank für Berlin...
Google Kalender
STRATO Kunden
In welchen Bereich möchten Sie sich
STRATO Kunden-Login
Webmail
HiDrive
Webshops
strato.de/apps/CustomerService#/skl
Burks' Blog
Kostenlos Schach o...
Die Bank für Berlin...
Google Kalender
FRITZ!Box
Webmail
HiDrive
Webshops
Login