

Was tun gegen Viren, Trojaner und Würmer?

Fortschreitende Technologie hilft uns, den Alltag zu erleichtern. Die wachsende Zahl der neuen Schadsoftware, auch Malware genannt, ist eine der unangenehmsten Entwicklungen der Technologie. Die Schadsoftware wird dauernd darauf optimiert, nicht von Antivirenprogrammen entdeckt zu werden. Sobald die Malware ausfindig gemacht wurde, ist bereits neue Schadsoftware im Umlauf.



Was sind Viren, Trojaner und Würmer?

Als Viren, Trojaner und Würmer bezeichnet man Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Sie alle gehören zur Gattung Schadsoftware. Ist ein Computer von Schadsoftware befallen, kann es sein, dass darauf lokal gespeicherte Daten nicht mehr vor unberechtigten Zugriffen geschützt sind.

Schadsoftware kann über E-Mails, Links auf Websites oder USB Sticks verbreitet werden. Da die Anzahl schädlicher E-Mails und schädlicher Software in den letzten Monaten weltweit stark zugenommen hat, wird es immer wichtiger, sich gut dagegen zu schützen.

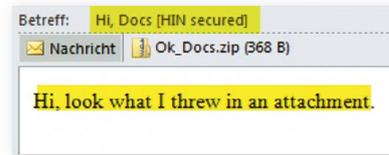
Wie schütze ich mich gegen Schadsoftware?

- Seien Sie vorsichtig bei verdächtigen E-Mails, selbst wenn diese von Ihnen bekannten Absendern stammen. Leider können Absenderadressen sehr einfach gefälscht werden.
- Löschen Sie verdächtige Nachrichten umgehend, ohne angefügte Dateien im Anhang zu öffnen.
- Löschen Sie die Nachricht auch im Papierkorb Ihrer E-Mail Ablage.
- Beachten Sie, dass auch mit [HIN secured] markierte E-Mails Schadsoftware enthalten können.
- Klicken Sie nie auf Links in verdächtigen E-Mails und öffnen Sie auch keine Anhänge.
- Verwenden Sie Ihr HIN-Passwort niemals für fremde Applikationen.
- Verwenden Sie Ihre HIN Mailadresse nur für geschäftliche Zwecke und achten Sie darauf, diese nicht unnötig oder entsprechend geschützt (z.B. felix.muster{at}hin.ch) zu publizieren.
- Halten Sie grundsätzlich Ihr System auf dem neuesten Stand (Browser, E-Mail-Programm, Virenschutzprogramm, Betriebssystem, Office etc.). Installieren Sie Updates immer umgehend, insbesondere, wenn es sich um Sicherheits-Updates handelt.
- Bei Windows PCs und Mac sind Virenschutzprogramme zwingend. Mac Systeme sind zwar seltener betroffen, aber ein Virenschutzprogramm erhöht die Sicherheit.
- Erstellen Sie regelmässig Backups von Ihren Systemen.

Woran erkenne ich schädliche E-Mails?

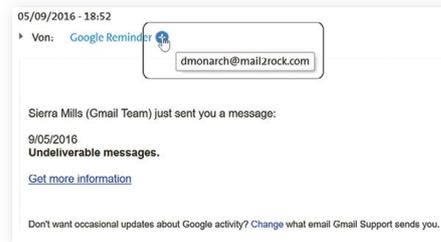
Gefährlicher Anhang

- Direkte Aufforderung, auf das Attachment zu klicken.
- Unpersönlich
- Englisch



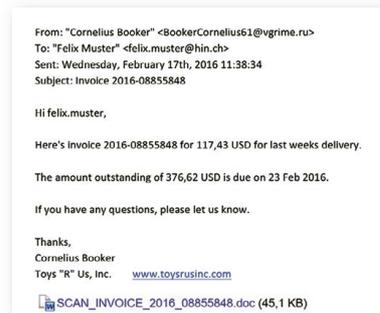
Vorgetäuschter Absender

- Der Absender eines Mails hat nichts mit der vorgetauschten Firma zu tun.
Achtung: E-Mail Absender lassen sich einfach fälschen, d.h. mit wenig Aufwand wäre eine etwas weniger offensichtliche Fälschung möglich, als im Beispiel dargestellt ist.



Fehlerhafte Anrede

- Der bekannte Teil der Mailadresse (felix.muster) wird mehrfach verwendet, aber nicht weiter personalisiert. Man kann herleiten, dass dem Absender nichts bekannt ist über den Empfänger oder was Nachname oder Vorname bedeutet.
- (Im beiliegenden Bild ist das Attachment aus Platzgründen nicht gezeigt)



Täuschende Links

- Links zeigen auf ganz andere Ziele als der vorgetauschte Absender (Achtung: Maus auf Link bewegen, aber auf keinen Fall klicken).
- Das Ziel des Links wird, je nach Programm, in der Fusszeile oder neben dem Link angezeigt.
- Diese Taktik wird häufig im Zusammenhang mit Phishing-Mails bei Banktrojanern verwendet.



Das Muster ist immer dasselbe, es wird mentaler Druck (z.B. offene Rechnung, Gewinnchance, Geschäftsidee, Bewerbung, vergessene Aufgabe, wichtige und dringende Aufgabe u.v.m.) erzeugt, das Attachment zu öffnen oder auf einen Link zu klicken.

- Mails auf Deutsch enthalten manchmal, aber weniger häufig als auch schon, Tipp- und Sprachfehler.
- Auch E-Mails von Ihnen bekannten Absendern können Schadsoftware enthalten, da sich diese unbemerkt über das lokale Adressbuch der Betroffenen verbreiten kann.
- Schadsoftware kann sich als unauffällige Datei im Anhang von E-Mails befinden, z.B. als zip, doc, pdf oder jpg Datei. Sobald diese Datei geöffnet wird, installiert sich die schädliche Software auf Ihrem Computer.

Was tun, wenn ich eine schädliche E-Mail oder eine schädliche Datei geöffnet habe?

- Trennen Sie Ihren Rechner vom lokalen Netzwerk, so können Sie vielleicht verhindern, dass weitere Rechner infiziert werden.
- Prüfen Sie Ihren Computer mit einem aktuellen Virenschutz-Programm.
- Kontaktieren Sie den HIN Support. Dieser kann abklären, ob Ihr Virenschutzprogramm die entsprechende Schadsoftware erkennt.
- Stellen Sie sicher, dass die Nachricht mit dem schädlichen Anhang auf keinem anderen Computer geöffnet wird. Informieren Sie dazu alle an den Arbeitsstationen tätigen Personen. Löschen Sie die Nachricht aus allen E-Mail-Konten (inkl. dem Papierkorb).
- Setzen Sie sich mit Ihrem IT-Partner in Verbindung.

Was tut HIN gegen Schadsoftware?

HIN steht für datenschutzkonforme elektronische Kommunikation und Interaktion. Dies bedeutet:

- Der Datenschutz bei HIN ist gewährleistet – «sicher» steht für «datenschutzkonform».
- HIN schützt vor fremdem Zugriff auf E-Mails und unberechtigtem Zugriff auf Applikationen.
- HIN E-Mails an andere HIN Teilnehmende werden automatisch verschlüsselt, so dass sie von Dritten weder eingesehen noch verändert werden können.

Datenschutz ist nicht gleich Virenschutz: Die Verschlüsselung der HIN E-Mails schützt nicht davor, dass Schadsoftware über HIN Mail verbreitet werden kann.

Das HIN Team arbeitet permanent daran, die Ausbreitung von Schadsoftware zu verhindern.

- Die HIN Plattform ist mit Schutzvorrichtungen wie einer Virenschutzsoftware und sogenannter Anti-Malware ausgestattet.

- Der HIN Virenschanner kontrolliert alle E-Mails darauf, ob sie Schadsoftware enthalten – egal ob sie von HIN Adressen oder von aussen kommen.
- Wird in einer E-Mail ein Virus erkannt, leitet HIN diese nicht an den Empfänger weiter.
- Viren- und Trojaner, resp. ganz grundsätzlich Cyberattacken stellen ein sehr hohes und oft nicht kalkulierbares Risiko dar.

Schadsoftware verändert sich im Sekundentakt, so dass selbst Virenschanner oft das Nachsehen haben resp. sich Schadsoftware unbemerkt und z.B. als E-Mail getarnt in Ihr System einnisten kann.

Aus diesem Grund kann auch die Health Info Net AG keine Verantwortung resp. Haftung für allfällige Schäden übernehmen.

Für das Kundensystem ist der Kunde selbst verantwortlich. Entsprechend ist es wichtig, die hier aufgeführten Hinweise zu befolgen.

Weitere nützliche Informationen und Fragen

- Stellen Sie Ihre Fragen in unserer Gruppe «Forum für Datensicherheit» auf HIN Home
Link auf: <http://community.hin.ch/groups/tipps-tricks-fragen-antworten/>
- Häufig gestellte Fragen finden Sie in unseren FAQ: www.hin.ch/schadsoftware
- Wir stehen Ihnen gerne zur Verfügung. Sie erreichen unseren HIN Calldesk von Montag bis Freitag von 08.00 bis 18.00 Uhr unter der Telefonnummer 0848 830 740 oder unter support@hin.ch.