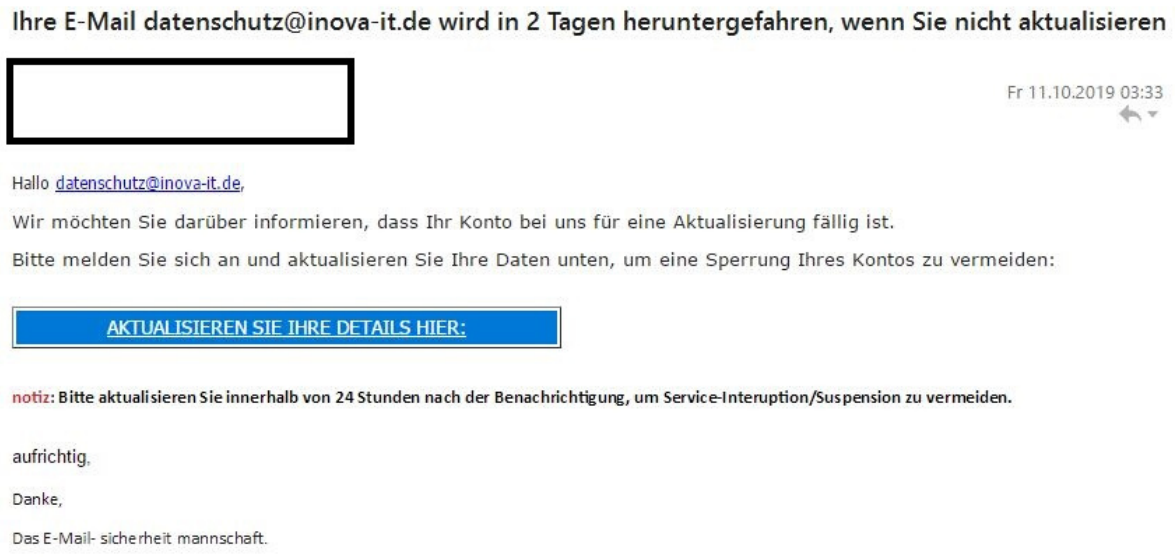
Merkmale einer Phishing-Mail und wie man sich dagegen schützen kann



Ihre E-Mail datenschutz@inova-it.de wird in 2 Tagen heruntergefahren, wenn Sie nicht aktualisieren

[redacted]

Fr 11.10.2019 03:33

Hallo datenschutz@inova-it.de,

Wir möchten Sie darüber informieren, dass Ihr Konto bei uns für eine Aktualisierung fällig ist.

Bitte melden Sie sich an und aktualisieren Sie Ihre Daten unten, um eine Sperrung Ihres Kontos zu vermeiden:

AKTUALISIEREN SIE IHRE DETAILS HIER:

notiz: **Bitte aktualisieren Sie innerhalb von 24 Stunden nach der Benachrichtigung, um Service-Interuption/Suspension zu vermeiden.**

aufrichtig,

Danke,

Das E-Mail- sicherheit mannschaft.

Gefälschte E-Mails, sogenannte Phishing Mails tauchen immer häufiger im Netz auf. Dabei wird versucht, dem Empfänger wichtige Daten zu stehlen. Auf den ersten Blick sehen diese E-Mails häufig täuschend echt aus. Genau das wird vielen Nutzern zum Verhängnis, wenn sie gutgläubig ihre sensiblen Daten angeben. So kann das Öffnen von Phishing-Mails nicht nur dazu führen, dass der Computer mit einem Virus infiziert wird, sondern es kann auch richtig Geld kosten.

Klicken Sie keine Links in der E-Mail an!

1. Wie erkennt man eine Phishing E-Mail?

Grammatik- und Rechtschreibfehler

E-Mails, die in einem fehlerhaften Deutsch geschrieben sind, sind am leichtesten zu durchschauen. Meistens wurden sie nicht in Deutsch verfasst, sondern mit einem Übersetzungsdienst aus einer anderen Sprache übersetzt worden. Weitere Hinweise auf solche E-Mails sind Zeichensatzfehler, wie etwa kyrillische Buchstaben oder auch fehlende Umlaute.

Mails in fremder Sprache

Ebenfalls schnell zu erkennen sind E-Mails, die auf Englisch oder Französisch verfasst worden sind. Sollte man nicht gerade Kunde einer Bank mit Sitz im Ausland sein, kann man sich sicher sein, dass man (wenn überhaupt) seine E-Mails von der Bank nur auf Deutsch bekommt.

Fehlender Name

Unternehmen sprechen in E-Mails grundsätzlich mit dem Namen des Empfängers an und niemals mit „Sehr geehrter Kunde“ oder „sehr geehrter Nutzer“. Sehr raffinierte Phishing-Täter haben aber oftmals auch schon den Namen herausgefunden und schreiben mit persönlicherAnsprache an, um der E-Mail eine höhere Glaubwürdigkeit zu verleihen.

Inova-iT

Dringender Handlungsbedarf

Man sollte ebenfalls stutzig werden, wenn man via E-Mail aufgefordert wird, ganz dringend und innerhalb einer bestimmten (meist kurzen) Frist zu handeln. Insbesondere, wenn diese Aufforderung mit einer Drohung verbunden ist – beispielsweise, dass sonst die Kreditkarte oder der Online-Zugang gesperrt werden.

Eingabe von Daten

Die Aufforderung, persönliche Daten sowie möglicherweise PIN oder TAN einzugeben, ist ein weiterer Hinweis. Banken oder Online-Zahlungsdienste werden um so etwas nicht per E-Mail bitten. PIN und TAN werden von Geldinstituten niemals telefonisch oder per E-Mail abgefragt, denn dies zählt zu den wesentlichen Sicherheitsregeln.

Links oder eingefügte Formulare

Unternehmen versenden in der Regel keine E-Mails, sondern Briefe. Falls man doch eine E-Mail erhält, werden diese keine Dateianhänge (wie Formulare, über die eine Eingabe gemacht werden muss) enthalten. Unternehmen versenden nur in Ausnahmefällen E-Mails mit Links, auf die der Empfänger klicken soll. Dann geht es beispielsweise um neue AGBs, niemals aber um das Einloggen in das Kundenkonto. Besser ist ohnehin, die Internetseite selbst aufzurufen.

Bisher noch nie eine E-Mail von diesem Unternehmen bekommen oder kein Kunde

Wenn ein Unternehmen nie bzw. selten E-Mails verschickt, eventuell die E-Mail-Adresse gar nicht kennen kann oder ein anderer Dienstleister versucht einem zu kontaktieren, mit den man gar keine Geschäftsbeziehung hat, sollte man die E-Mail löschen.

Mailheader

Um letzte Zweifel aufzuräumen sollte man sich den sogenannten Mail-Header anschauen. Dort steht die IP-Adresse des Absenders. Nur diese ist fälschungssicher und gibt Aufschluss über den tatsächlichen Absende

2. Wie kann man sich selber und andere schützen?

Absender kontrollieren:

Der Schutz vor Phishing-Mails kann nie zu 100% gewährleistet sein. Allerdings kann man versuchen, den Schaden möglichst einzudämmen. Das heißt, keine E-Mails öffnen, wenn man den Absender nicht kennt. Bei dem Erhalt einer verdächtigen E-Mail sollte man die E-Mail-Adressen der Verfasser blockieren, so kann man keine weiteren E-Mails von diesen Betrügern mehr bekommen. Und selbst wenn die E-Mail scheinbar von einem Bekannten oder Freund kommt: Scheint etwas merkwürdig zu sein, dann lieber Finger weg! Am besten die betreffende Person fragen, ob die verdächtige Nachricht tatsächlich von ihm stammt.

Links überprüfen

Wenn eine E-Mail einen Link enthält, sollte man dessen Adresse prüfen, bevor man sie öffnet. Indem man mit der rechten Maustaste auf eine Verlinkung klickt, wird unter anderem angezeigt, wohin der Link leitet. Achtung: der Link kann auch auf eine Phishing-Webseite leiten. Die Adresse dieser gefälschten Webseite sieht dann fast aus wie eine echte, seröse Seite. Aber eben nur fast. Deshalb sollte man bei verdächtigen E-Mails lieber zwei Mal hinschauen, als dass man Opfer eines Betruges wird. Wenn die angegebene Adresse sicher aussieht, trotzdem nicht auf den Link klicken. Hier sollte man die Adresse lieber selbstständig in ein neues Browser-Fenster eingeben, um sicherzugehen, dass der vermeintliche Link nicht doch auf eine andere Seite weiterleitet. Auch bei Eingabe sensibler Daten auf der Webseite, sollte man auf eine sichere Verbindung achten. Diese wird mit einem „s“ hinter dem http in der Header-Zeile angezeigt.

Gefälschte E-Mails betroffenen Unternehmen melden

Bei der Vermutung, eine gefälschte E-Mail eines bekannten Unternehmens bekommen zu haben, sollte man dieses Unternehmen kontaktieren. Einerseits kann man dadurch sichergehen, dass die E-Mail tatsächlich von diesem Verfasser stammt – oder eben nicht.
Andererseits wird so dem Unternehmen mitgeteilt, dass in seinem Namen gefälschte E-Mails versendet werden. So bietet zum Beispiel Amazon eine Anleitung an, wie mit gefälschten E-Mails umgegangen werden sollte. Denn solche betrügerischen E-Mails können einem Unternehmen ganz schön schaden – selbst wenn es mit dem Betrug gar nichts zu tun hat.

Immer gesicherte Netzwerke benutzen

Wenn man persönliche Daten im Internet handhaben will: immer über ein gesichertes Netzwerk einloggen! Dazu zählt beispielsweise das eigene Heimnetzwerk. Öffentliche WLAN-Verbindungen, wie beispielsweise in Restaurants oder Flughäfen sollten nie für die Verarbeitung sensibler Daten verwendet werden. Denn Achtung: Jeder kann in einem solchen Netzwerk herumpfuschen.

Daten vom Original-Anbieter prüfen lassen

Am besten sollte man sämtliche Zugangsdaten, wie Nutzername und Passwort ändern. Wenn der PC Teil eines Phishing-Angriffs geworden ist und einen Passwortmanager auf dem PC installiert worden ist, steht Arbeit bevor: ändern sämtlicher Passwörter, die auf dem Manager abgespeichert sind. Auch das Benutzen einer Antiviren-Software erweist sich als ratsam. Diese kann Viren-Angriffe durch Phishing-Mails gezielt abwehren.