Infoblatt als Hilfestellung für den sicheren Umgang mit E-Mails

Auch wenn Virenscanner und Spamfilter eingesetzt werden, kann es sein, dass Phishing-Mails „durchrutschen" und neueste Schadsoftware noch nicht erkannt wird.

Beispiele dafür finden sich in den Medien regelmäßig, vor wenigen Tagen erst hat die Ransomware „WannaCry" großen Schaden angerichtet.

Internet-Kriminalität, Ransomware etc. ist ein globales Geschäftsmodell mit dem Milliarden umgesetzt werden!

Es ist daher wirklich wichtig beim Umgang mit Mails Vorsicht walten zu lassen! Dieses Infoblatt soll Ihnen dabei helfen „verdächtige Mails" zu erkennen.

Wie erkenne ich „böse Mails"?

- Am Absender.
  Ist mir dieser ganz und gar unbekannt, kann ich schon einmal vorsichtiger sein.

- Wenn der Betreff ebenfalls keinen Sinn ergibt, kann ich mich ev. schon entscheiden das Mail zu löschen.
  Habe ich z.B. keinen Account bei der Deutschen Telekom, dann brauche ich das Mail mit dem Betreff „Rechnung" oder „Mahnung" gar nicht erst aufzumachen.

- Entscheide ich mich das Mail zu öffnen, bekomme ich mehr Informationen. z.B. sehe ich beim Absender auch die dahinterstehende Mail-Adresse (siehe Bild-Beispiele am Ende).
  Passt diese nicht zum angezeigten Absender-Namen, ist es mit an Sicherheit grenzender Wahrscheinlichkeit ein Fake.

- Geht das Mail (von meiner Bank, Paypal, etc.) an mehrere Empfänger (die mir angezeigt werden) ist das ebenfalls ein sicherer Hinweis vorsichtig zu sein.

- An Grammatik und Rechtschreibung.
  Kommt das Mail vermeintlich von einem großen Konzern, und ist aber voll von Fehlern wird es nicht echt sein.

- Werde ich aufgefordert, Informationen über mein Konto auf einer Website einzugeben bzw. mein Konto zu bestätigen etc. ist es auch mit Sicherheit ein Fake. Kein seriöser Anbieter wird seine Nutzer per Mail dazu auffordern.

Franz F. Klein - Informationstechnologie

Web http://www.ffk.co.at
E-Mail office@ffk.co.at

- Ich kann mir die Links, die in dem Mail vorhanden sind, bevor ich sie anklicke „ansehen".
  Wenn ich mit der Maus vor dem Anklicken über dem Link-Text stehen bleibe, sehe ich die tatsächliche Internet-Adresse die dahintersteht.
  Meist offenbart sich spätestens hier die böse Absicht (siehe Bild Beispiele am Ende).

- Ist dem Mail ein HTML-Formular beigefügt, dass ich ausfüllen soll, steht ebenfalls sicher böse Absicht dahinter.

- Soll ich die Rechnung/Mahnung/… herunterladen, und der Link führt zu Dateien mit den Endungen.pdf.zip oder .exe.zip, oder direkt zu .exe ist es sicher auch Schadsoftware. Auch hier wieder: Mit der Maus über dem Link-Text stehenbleiben und abwarten wie die tatsächliche Adresse aussieht.

- Wenn die Rechnung (o.ä.) in einer zip-Datei verpackt ist, und mir im Text ein Kennwort genannt wird, das ich zum Entpacken der zip-Datei brauche, ist ebenfalls sicher Schadsoftware. (Die kennwortgeschützte zip-Datei hindert Virenscanner daran, den Inhalt zu scannen)

- Attachments mit Endungen wie .exe, .cmd, .ps, .hta, .vbs, …
  (ausführbare Dateien) sollten Sie nie öffnen!

- Aber auch in Word und PDF Dateien kann Schad-Code versteckt sein.
  Man muss daher auch bei diesen Dateien vorsichtig sein.

Kurz zusammengefasst:

- Immer auf Plausibilität prüfen!
  - Ist es wahrscheinlich, dass mir dieser Absender etwas schickt? (Beispiel: „Deutsche Telekom")
  - Habe ich eine Geschäftsbeziehung mit dem Absender? (Beispiel: Betreff „Ihre Rechnung")
  - Stimmt die Aufmachung des Mails? (Layout, Rechtschreibung/Grammatik, Signatur)
- Links überprüfen, bevor man sie anklickt!
- Zweimal nachdenken, bevor man Attachments öffnet!
- Sicherheitswarnungen des E-Mail-Programms und des Betriebs-Systems ernst nehmen! Warn-Dialoge wirklich lesen und überdenken, bevor man sie bestätigt!

Franz F. Klein - Informationstechnologie

Web http://www.ffk.co.at
E-Mail office@ffk.co.at

Begriffe:

- Phishing:
  Kunstwort aus Password und Fishing = Phishing.
  Also „Angeln nach Passwörtern".
  Es wird versucht den Benutzer durch täuschend echt (manchmal auch grottenschlecht) aussehende Mails zu verleiten, seine Zugangsdaten auf einer „Fake-Site" einzugeben. Zielt z.B. auf Telebanking/Netbanking aber auch auf PayPal, Facebook, Firmen-Accounts und andere Accounts ab.

- Spear-Phishing
  Individuell angepasste Phishing Mails (auf Basis von verfügbaren Informatioen von der Firmen-Homepage, Facebook, LinkedIn und anderen Medien) um die Wahrscheinlichkeit zu erhöhen, dass der Empfänger Informationen preisgibt.

- Virus:
  Recht allgemeiner Begriff für Schadprogramme.
  Viren, die „einfach nur" Schaden anrichten, sind extrem selten geworden.
  Viel häufiger sind Varianten die den PC über lange Zeit ausspähen oder in ein Botnet eingliedern, um Angriffe zu führen.

- Ransomware:
  Schadsoftware, die den PC sperrt, und für die Entsperrung Geld verlangt (z.B. per nicht nachvollziehbarer paysafecard oder ukash etc.).

  Manche bauen dabei sogar passende Polizei/Innenministeriums-Logos ein (auch österreichische) und behaupten, dass illegale Inhalte gefunden wurden.Die Strafe kann dann gleich online beglichen werden, um den PC zu entsperren.

  Im Gegensatz dazu offenbaren andere die kriminelle Absicht sofort und erpressen Geld um die vom Virus verschlüsselten Dateien des Benutzer zu entschlüsseln.

- Scareware:
  Programme die sich z.B. als Antivirus Programm ausgeben, jede Menge vermeintliche Viren finden, den PC meist ziemlich unbedienbar machen, und dann z.B. 49,00 EUR für das Upgrade auf die Antivirus-Pro Variante verlangen, die alle (vermeintlichen) Viren und Probleme beseitigen kann.

- Trojaner:
  Ein Programm (ein „Virus"), das eingeschleust wird, um Daten und Aktivitäten auf dem PC auszuspähen. Oft auch mit Keyloggern ausgestattet, die alle Tastatureingaben (also auch Kennwörter etc.) mitschreiben.

- Wurm:
  Ein Programm (ein „Virus"), das die Fähigkeit hat, sich selbst über Netzwerke zu verbreiten. Oft werden dafür bekannte und unbekannte Sicherheitslücken ausgenutzt (auch sogenannte „Zero Day Exploits").

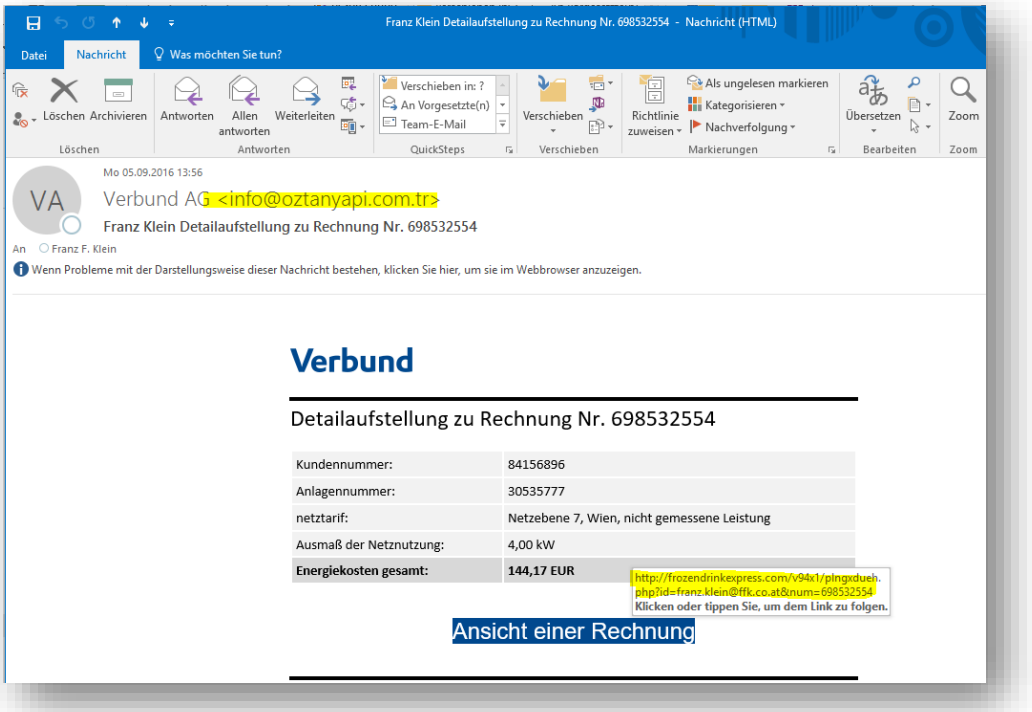
- Botnet:
  Ein Netzwerk aus infizierten PCs, das unter Kontrolle von Kriminellen steht. Diese PCs werden dann z.B. für Angriffe auf andere PCs/Server/Webseiten benutzt. Da Botnets durchaus mehrere zehntausend PCs umfassen können, sind die damit durchgeführten Angriffe entsprechend massiv. Der Benutzer bekommt meist nicht mit, dass sein PC infiziert ist und dafür missbraucht wird.

Franz F. Klein - Informationstechnologie

Web http://www.ffk.co.at
E-Mail office@ffk.co.at

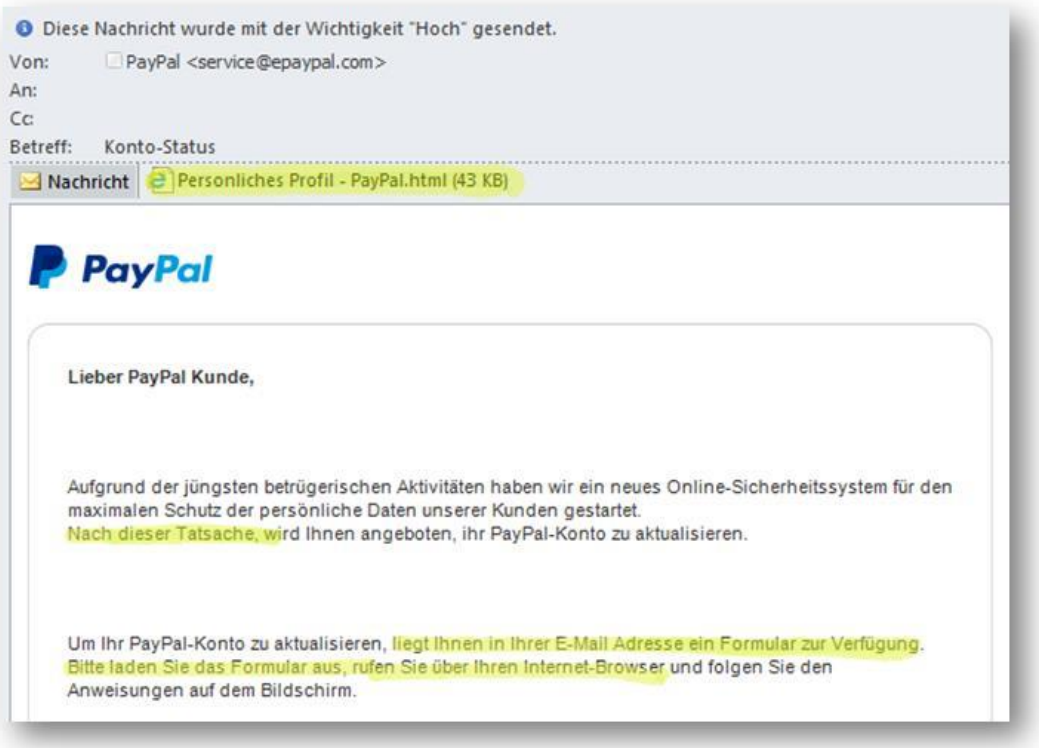
Bild-Beispiele:

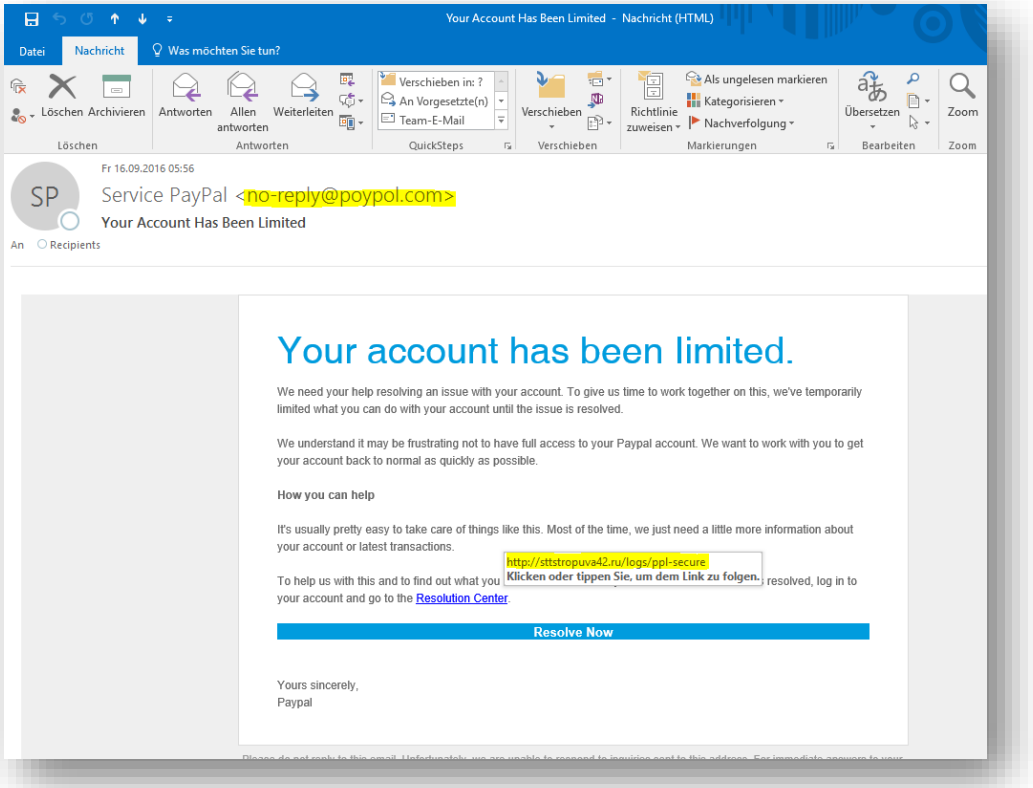
(„Auffälligkeiten" sind gelb markiert)



Franz F. Klein - Informationstechnologie

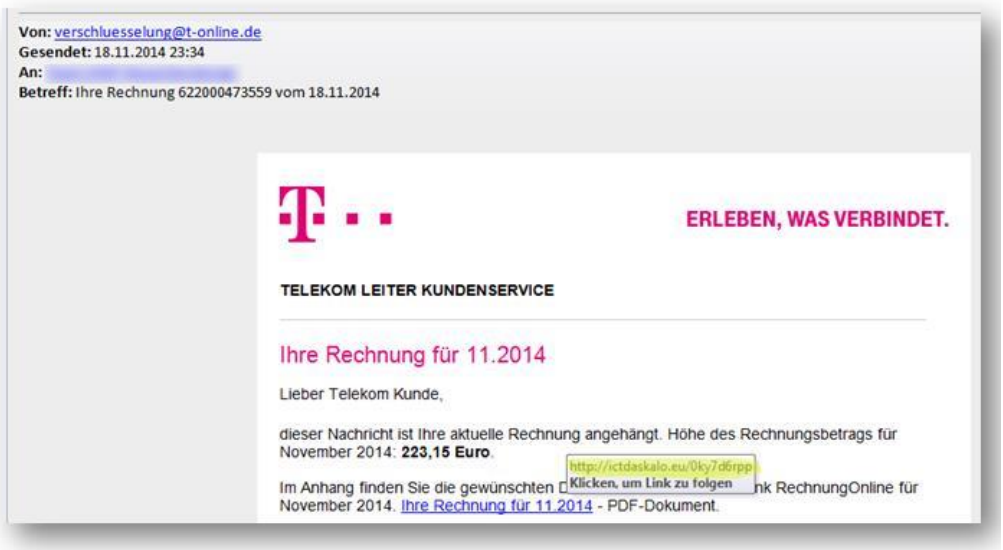
Web http://www.ffk.co.at
E-Mail office@ffk.co.at





Franz F. Klein - Informationstechnologie

Web http://www.ffk.co.at
E-Mail office@ffk.co.at



Von: verschluesselung@t-online.de
Gesendet: 18.11.2014 23:34
An:
Betreff: Ihre Rechnung 622000473559 vom 18.11.2014

ERLEBEN, WAS VERBINDET.

TELEKOM LEITER KUNDENSERVICE

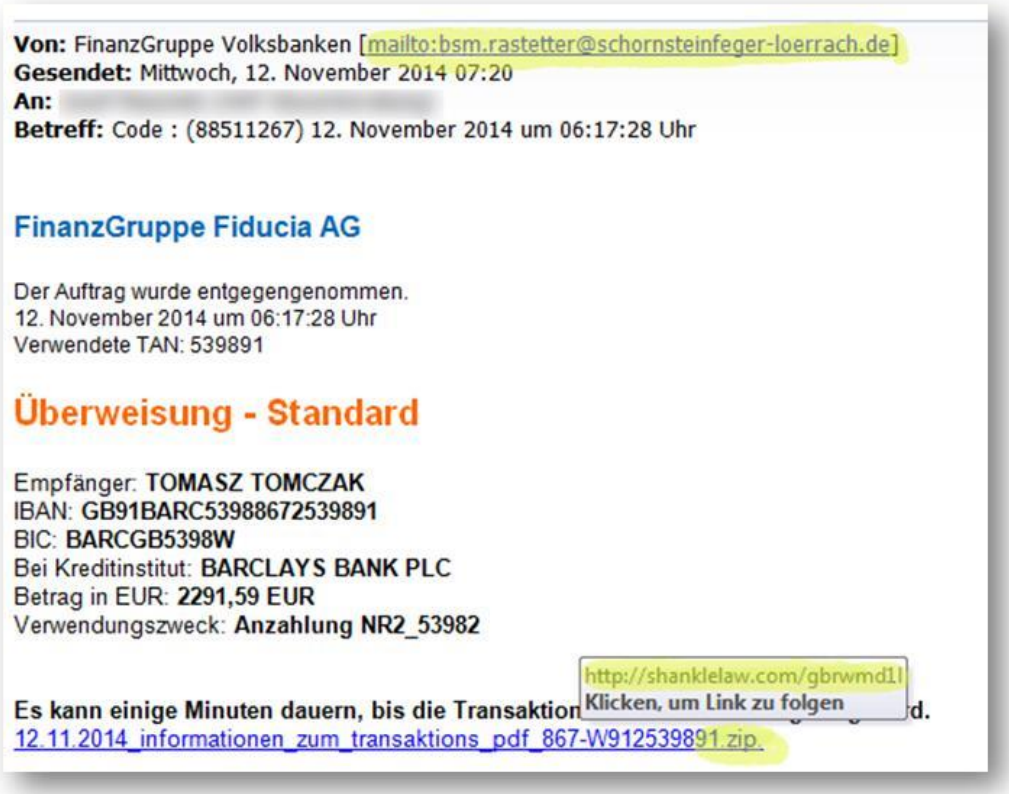
Ihre Rechnung für 11.2014

Lieber Telekom Kunde,

dieser Nachricht ist Ihre aktuelle Rechnung angehängt. Höhe des Rechnungsbetrags für November 2014: **223,15 Euro**.

http://ictdaskalo.eu/0ky7d6rpp
Klicken, um Link zu folgen

Im Anhang finden Sie die gewünschten [illegible]nk RechnungOnline für November 2014. Ihre Rechnung für 11.2014 - PDF-Dokument.



Von: FinanzGruppe Volksbanken [mailto:bsm.rastetter@schornsteinfeger-loerrach.de]
Gesendet: Mittwoch, 12. November 2014 07:20
An:
Betreff: Code : (88511267) 12. November 2014 um 06:17:28 Uhr

FinanzGruppe Fiducia AG

Der Auftrag wurde entgegengenommen.
12. November 2014 um 06:17:28 Uhr
Verwendete TAN: 539891

Überweisung - Standard

Empfänger: **TOMASZ TOMCZAK**
IBAN: **GB91BARC53988672539891**
BIC: **BARCGB5398W**
Bei Kreditinstitut: **BARCLAYS BANK PLC**
Betrag in EUR: **2291,59 EUR**
Verwendungszweck: **Anzahlung NR2_53982**

http://shanklelaw.com/gbrwmd1l
Klicken, um Link zu folgen

Es kann einige Minuten dauern, bis die Transaktion [illegible]d.
12.11.2014_informationen_zum_transaktions_pdf_867-W912539891.zip

Franz F. Klein - Informationstechnologie

Web http://www.ffk.co.at
E-Mail office@ffk.co.at

Franz F. Klein - Informationstechnologie

Web http://www.ffk.co.at
E-Mail office@ffk.co.at