

Phishing Mails



Vortrag abgelegt unter: VG-Pellenz / Bürgerservice / Digitalbotschafter / Downloads

Datenschutz im Internet

Herbert Hagenau

Digi-Hilfe-Treff



VG Pellenz

Digital-Botschafter RLP

Ministerium RLP Sozial..Digitales

Alexander Schweitzer / Sabine Bätzing-Lichtenthäler



Phishing Mails

- **Das Wichtigste in Kürze:**

- Betrügerische E-Mails sind oft täuschend echt

- Wenn man es nicht einschätzen kann

Beim Absender nachfragen

Aber Achtung:

Nicht direkt auf die verdächtige E-Mail antworten

- Wenn E-Mail ein Betrugsversuch ist

Keine Links anklicken und keine Dateianhänge öffnen

- Löschen Sie die E-Mail

Sperren der Absenderadresse, als Spam markieren

Phishing Mails

Die wichtigsten Merkmale einer Phishing Mail

- **Grammatik- und Orthografie-Fehler**

Fehlerhaftes Deutsch, Zeichensatzfehler, kyrillische Buchstaben oder fehlende Umlaute

- **In fremder Sprache geschrieben**

Man bekommt (wenn überhaupt) E-Mails von Ihrer Bank nur auf Deutsch

- **Name fehlt in der Anrede**

"Sehr geehrter Kunde" oder "Sehr geehrter Nutzer".

- **Gut zu wissen:**

Phishing-Täter haben evtl. ihren Namen und nutzen persönliche Ansprache
Kriminelle versuchen, der E-Mail eine höhere Glaubwürdigkeit zu verleihen.

Phishing Mails

- **Woher haben die Kriminellen Ihre Daten?**

Viele Möglichkeiten. Anbieter gehackt, Zu Daten Freigabe , Dritte Daten"abgefischt", Trojanisches Pferd oder Schadprogramm

- **Wann besteht dringender Handlungsbedarf**

via E-Mail aufgefordert, ganz dringend und innerhalb kurzer Frist

- **Insbesondere, bei einer Drohung**

Kreditkarte oder Online-Zugang gesperrt werden.

- **Sie sollen Daten eingeben**

persönliche Daten sowie PIN oder TAN einzugeben.

- **Sie sollen eine Datei öffnen**

Datei zu öffnen, als Anhang oder direkt in der Mail, einen Link

- **Keinesfalls herunterladen oder gar öffnen.**

schädliches Programm, Virus oder ein trojanisches Pferd

Phishing Mails

- **Grundsätzlich misstrauisch sein.**

Links nicht anklicken, keine Formulare ausfüllen

- **Internetseite selbst aufrufen,**

Direkt im Adressfeld des Browsers eintippen.

- **Virenschutz-Programme**

Karlsruher Institut für Technologie (KIT) Tool "Torpedo"
Add-On, das für Chrome und Firefox und E-Mail-
Programm Thunderbird

Phishing Mails

- **Kein Kunde oder keine Kundin**

E-Mails von einer Bank oder andere Dienstleister, die man gar nicht kennt

Folgende Szenarien sind üblich:

- Ware, die Sie nie bestellt haben
- Änderungen an Verträgen
- Gebühren für Kreditkarten
- mehrfach Mahnschreiben
- mit Inkasso-Unternehmen gedroht

Löschen Sie all diese E-Mails.

- Wenn schon ein schädlicher Link geklickt oder eine Datei geöffnet wurde löschen Sie die Mail nicht, sie ist Beweismittel für die Polizei

Email weiterleiten an phishing@verbraucherzentrale.nrw

Phishing Mails

- **Prüfen Sie, ob der Absender vertrauenswürdig ist**
Auch Absenderangaben von E-Mails lassen sich fälschen.
- **Prüfen des sogenannten Mail-Header**
Dort steht die eindeutige IP-Adresse des Absenders
 - „ Nur diese ist fälschungssicher und gibt Aufschluss über den tatsächlichen Absender.
- **Achten Sie auf die Empfänger-Adresse**
Steht da nicht Ihre, ist das ein Warnsignal
- **Seriöse Newslettern oder E-Mails von Unternehmen**
Ihre eigene E-Mail-Adresse im An-Feld
- **Kriminelle nutzen auch das Feld BCC (Blindkopie)**
E-Mail an viele Empfänger gleichzeitig, ohne AdressAnzeige

Phishing Mails

- **Text E-Mail grundsätzlich ungefährlicher**

Bei reinen Text-E-Mails, die Sie im Browser oder mit einem E-Mail-Programm öffnen, kann nichts passieren, solange Sie nicht auf Links oder Anhänge klicken.

- **E-Mails im sogenannten HTML-Format**

Hier können nicht nur im Link oder im Anhang, sondern im Quellcode Schadprogramme hinterlegt sein.

Dann kann schon ein Klick auf eine Grafik in der E-Mail gefährlich sein

Evtl. deaktivieren des HTML-Formates

Phishing Mails

- **Wie erkenne ich eine Phishing-E-Mail?**

Meist ist eine Phishing-E-Mail so aufgebaut:

- Anrede,
- Grund der Mailverschickung
- Notwendigkeit zum Handeln
- Zeitdruck
- Konsequenzen, wenn Sie nicht handeln
- Link oder alternativ Dateianhang

Lieber einmal zu oft misstrauisch sein

Phishing Mails

- **Keine Links klicken oder Anhänge öffnen**

- **Nicht auf die E-Mail Antworten**

Dadurch verraten Sie Betrügern, dass diese E-Mail-Adresse regelmäßig genutzt wird

- **Wichtig:**

Auch bei einer namentlichen Anrede oder echt wirkenden Logos nicht sicher sein

Kriminelle bauen täuschend echt nach

Phishing Mails

- **E-Mail von meiner Bank, ob die E-Mail echt ist?**

Fragen Sie beim echten Anbieter nach.

- **Keine Kontaktmöglichkeit nutzen, die in der E-Mail angegeben ist.**

Suchen Sie besser eine Kontaktmöglichkeit auf der echten Internetseite des Anbieters.

Phishing Mails

- **Wie reagiere ich auf eine unberechtigte Forderung**

Seriöse Anbieter schicken Forderungen und insbesondere Mahnungen in der Regel per Post.

- **Grundsätzlich zwei Szenarien:**

- Der Text zielt darauf ab, auf einen Link klicken oder eine Datei zu öffnen.

- Jemand will tatsächlich Geld von Ihnen.

Eine konkrete Bankverbindung genannt ist genannt

Phishing Mails

- **Auf den Link in einer Phishing-E-Mail geklickt.**

Auch wenn Sie "nur" auf einen Link klicken, ohne auf der präparierten Internetseite Daten preiszugeben

- **Das sollten Sie als nächstes tun:**

- Virenschutzprogramm Aktualisieren
- Gesamten Computer untersuchen lassen.
- Automatischen Updates zulassen
- Experten hinzu ziehen.
- Entfernung von Schadsoftware

- **Evtl. persönliche PIN, Passwörter ändern**

Bei Dateneingabe nach der Schadprogramm-Installation
Bank informieren, falls das Online-Banking betroffen ist

Phishing Mails

- **Auch schon persönliche Daten eingegeben.**

Diese Daten sind jetzt in den Händen von Kriminellen

- **Adresse und Telefonnummer?**

Vorsichtig, wenn Sie demnächst Post bekommen oder Anrufe entgegennehmen

- **PIN, Passwort, Kontonummer oder Kreditkartennummer?**

- Kontaktieren Sie sofort Ihre(n) echten Anbieter, etwa das Kreditinstitut oder den Zahlungsdienstleister!
- Sperren Sie wenn nötig Konten oder Karten, zum Beispiel über die Sperr-Hotline 116 116!
- Ändern Sie umgehend Passwörter und Sicherheitsfragen!
- Bleiben Sie auf keinen Fall untätig!
- Prüfen Sie besonders regelmäßig Ihre Kontoauszüge!
- Stellen Sie [Strafanzeige bei der Polizei!](#)

- **Haben Cyber-Kriminelle weitere Zugänge erbeutet haben?**

Hilfe auf Webseiten des [Hasso Plattner-Instituts](#), der [Universität Bonn](#) und der [Seite des Sicherheitsforschers Troy Hunt](#)

Phishing Mails

Was kann ich gegen den Erhalt solcher E-Mails tun?

- Spam-Filter
- Daten-Sparsamkeit
- Unterschiedliche E-Mail-Adressen nutzen
- befallene E-Mail-Adresse löschen

Phishing Mails

Datenschutz im Internet

Phishing Mails

ENDE

Danke für ihre Aufmerksamkeit