Freie Universität Berlin

{tip4u://183} Version 1

Zentraleinrichtung für Datenverarbeitung (ZEDAT)
www.zedat.fu-berlin.de

Phishing Mails

Gefälschte E-Mail-Nachrichten sind ein Ärgernis und können ein hohes Sicherheitsrisiko darstellen. Dieses Merkblatt versucht zu erklären, woran diese erkannt werden können und wie mit ihnen umgegangen werden sollte.

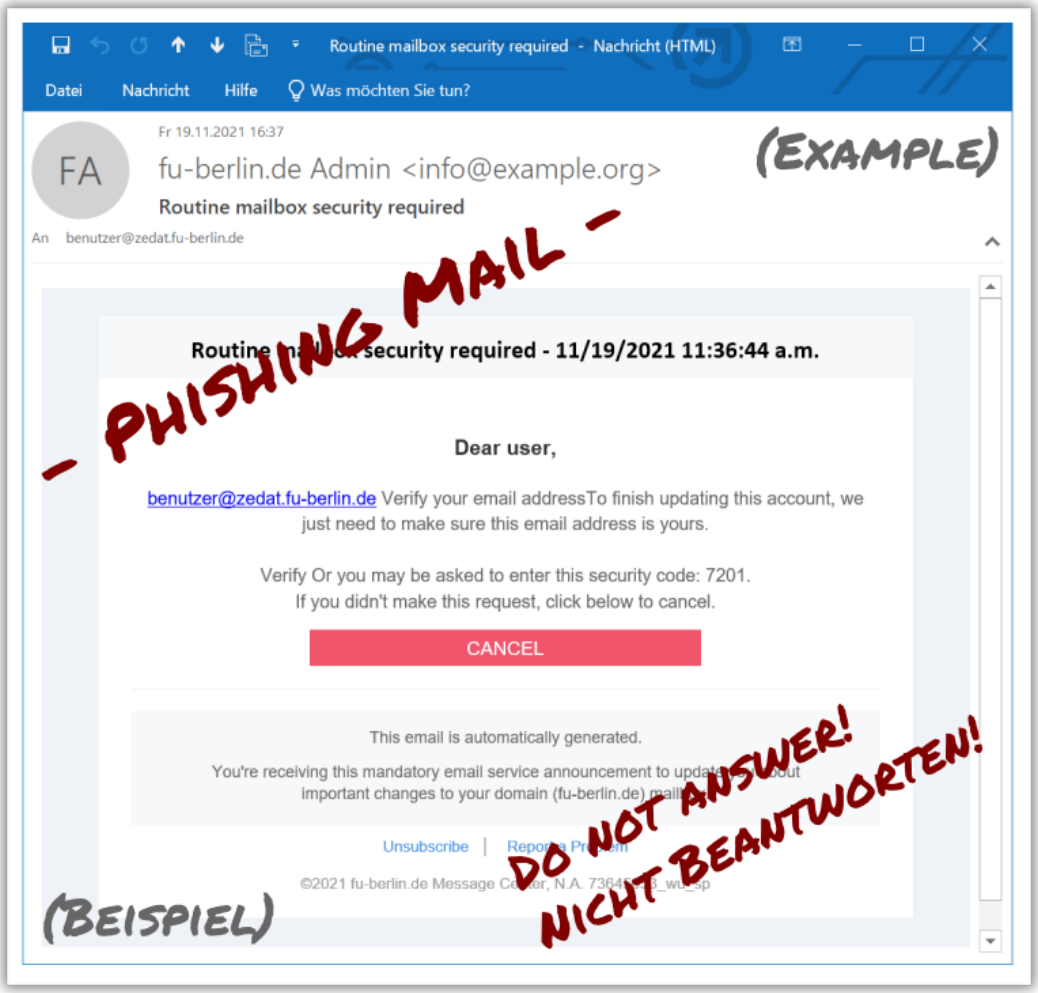
zedat

Zentraleinrichtung für Datenverarbeitung
Fabeckstraße 32 / 14195 Berlin
Hotline (030) 838 77777 / hilfe@zedat.fu-berlin.de

Gefälschte E-Mails (Phishing Mails)

Gefälschte Nachrichten sind ein inzwischen leider allgegenwärtiges Phänomen bei der E-Mail-Kommunikation. Das Kunstwort „Phishing“ (vom gleichklingenden englischen Begriff „fishing“ = Angeln) hat sich dabei für Angriffe eingebürgert, die genau das versuchen: das Fischen im Trüben nach unaufmerksamen Opfern. Einige Phishing Mails sind recht leicht zu identifizieren und viele davon werden schon automatisch in den eigenen Spam-Ordner einsortiert worden sein. Bei anderen ist es schwieriger, den Angreifern auf die Schliche zu kommen. **In allen Fällen gilt, dass erhöhte Aufmerksamkeit und gesundes Misstrauen der beste Schutz vor Trickbbetrügereien sind.**

Phishing Mails gibt es sowohl auf Englisch als auch auf Deutsch, und sie sollten auf gar keinen Fall beantwortet oder die darin enthaltenen Links angeklickt werden.



Ziel des Spiels

Phishing ist eine Form des sogenannten „Social Engineering“. Dabei wird versucht, über gefälschte E-Mails, aber auch über andere Kanäle wie Webseiten, Kurznachrichten, Anrufe o.ä. den Kommunikationspartner zu täuschen und in der Regel dazu zu veranlassen, persönliche Zugangsdaten zu verraten. Am Ende sind damit dann die Angreifer in der

Lage, auf diverse Ressourcen zuzugreifen und im Namen des Opfers zu agieren. Besonders prekär ist es, dass über einen auf diese Weise gekaperten Account oft sofort wieder neue Phishing Mails verschickt werden (gerne z.B. an alle Kontakte im Adressbuch), aber natürlich können auch Daten abfließen und anderes Unheil angerichtet werden.

Eine spezielle Abart von Phishing Mails ist der sogenannte „CEO Fraud". Es geht dabei darum, die Opfer durch psychologische Tricks dazu zu bringen, Geschenkkarten zu erwerben. Dadurch werden die Opfer direkt und persönlich finanziell geschädigt. Tip4U #184[1] beschreibt diese Form des Trickbetrugs im Detail.

Merkmale von Phishing Mails

Auch wenn Nachrichten auf den ersten Blick „ganz echt" aussehen, gibt es bei gefälschten E-Mails häufig Merkmale, die Empfängerinnen und Empfänger hellhörig werden lassen sollten. Kontrolliert werden kann unter anderem:

- Empfänger-Adresse
  - Warum habe ich die Mail bekommen?
  - Ist meine Adresse aufgeführt und wenn ja, ist es (wenn ich mehrere verwende) tatsächlich diejenige, die ich bei dem vermeintlichen Absender angegeben habe?
- Absender-Adresse
  - Stammt die Mail tatsächlich vom vermeintlichen Absender?
  - Für Mail-Profis: Passen die Headerzeilen zu dem, was ich erwarten würde?
  - Stimmen Name und E-Mail Adresse?
  - Ist die Domain (der Teil hinter dem „@"-Zeichen) korrekt oder sieht sie nur auf den ersten schnellen Blick „so ähnlich" aus?
  - Falls ich den Absender kenne und alles korrekt aussieht: Könnte es sein, dass sein Konto gehackt wurde?
- Betreff
  - Gibt es einen leeren, sinnlosen oder nichts-sagenden Betreff?
  - Gibt es einen reißerischen oder sich (zu) dringend-machenden Betreff?
  - Ist der Betreff in der Sprache, die ich bei dem Absender erwarten würde?
- Anrede
  - Gibt es überhaupt eine persönliche Anrede?
  - Stimmt die Anrede mit dem überein, was ich erwarten würde?
- Inhalt und Formatierung
  - Passt die Formatierung der Mail zu dem, was ich erwarten würde?
  - Für Mail-Profis: Gibt es eine alternative (Nur-Text) Version der Nachricht, die ich kontrollieren kann?
  - Passen Rechtschreibung und Grammatik?
  - Sind Probleme bei der Darstellung (z.B. auch bei Sonderzeichen oder Umlauten) zu erkennen?
  - Besteht die Mail aus einem Gemisch von Deutsch und Englisch?

[1] https://zedat.fu-berlin.de/tip4u_184.pdf

  - Passt die Grußformel zu dem, was ich erwarten würde?
  - Gibt es Unregelmäßigkeiten oder andere Auffälligkeiten?

- Knackpunkte
  - Wozu genau möchte mich die Mail überreden?
  - Gibt es eine Aufforderung zur Bestätigung meiner Zugangsdaten?
  - Soll ich mich irgendwo „legitimieren“ und als „Beweis“ Benutzernamen und Passwort eingeben?
  - Wird dafür ein knapper Zeitrahmen gesetzt?
  - Wird mit der Löschung von Mails oder Daten bzw. der Deaktivierung des Kontos gedroht?
  - Gibt es Links auf (dubiose) Websites?
  - Wird versucht, mir weiszumachen, mein Konto sei defekt oder gehackt worden?

Unter anderem diese Punkte können ein Indiz dafür sein, dass es sich um eine betrügerische Nachricht handelt. Natürlich versuchen die Angreifer immer, den Anschein größtmöglicher Seriosität zu erwecken und die Mails möglichst ansprechend zu gestalten. Parallel wird häufig versucht, Druck aufzubauen. Gerne wird dabei vorgegaukelt, dass es nötig sei, in kürzester Zeit zu reagieren und die eigenen Zugangsdaten irgendwo anzugeben. Drohungen wie die Sperrung des Kontos oder Datenverlust runden das Bild ab.

Phishing Mail im Posteingang – was tun?

Im Laufe eines E-Mail-Lebens landet mit hoher Wahrscheinlichkeit die eine oder andere Phishing Mail im eigenen Postfach.

Wer solch eine betrügerische Nachricht im eigenen Spam-Ordner findet, tut gut daran sie dort zu belassen, denn da ist sie schon genau an der richtigen Stelle.

Hat es eine Phishing Mail in den normalen Posteingang geschafft, sollte diese am besten einfach gelöscht werden. Nichts ärgert einen Phisher mehr, als wenn er nichts am Haken hat.

Ist nicht sicher, ob eine Mail echt oder eine Fälschung ist, kann z.B. beim Absender nachgefragt werden, ob er tatsächlich die fragliche Nachricht verschickt hat. Sicher ist sicher. Dies sollte natürlich am besten nicht per E-Mail, sondern auf anderem Wege, z.B. per Telefon (wobei die Nummer tunlichst nicht der fragwürdigen Nachricht entnommen werden sollte) erfolgen. In Zweifelsfällen sind das IT-Personal des eigenen Bereichs oder die Hotline der ZEDAT gute Ansprechpartner, die mithelfen können, die Echtheit zu bewerten. Kontaktmöglichkeiten der ZEDAT-Beratung finden sich unter:

https://www.zedat.fu-berlin.de/Beratung

Auf keinen Fall sollten (potenzielle) Phishing Mails beantwortet oder darin enthaltene Links angeklickt werden.

Was tun, wenn ich auf einen Betrug hereingefallen bin?

Erste Hilfe

Wer auf eine Phishing Mail hereingefallen ist und damit seine Zugangsdaten Dritten verraten hat, sollte umgehend das Passwort zum eigenen Account ändern! Am schnellsten

und einfachsten geht das i.d.R. über das ZEDAT-Portal unter:

https://portal.zedat.fu-berlin.de

Wenn die Kriminellen sich mit den erbeuteten Zugangsdaten nicht (mehr) anmelden können, ist der Angriff vereitelt.

Nachwirkungen

Eine Meldung an die IT-Kolleg:innen des eigenen Bereichs oder das Abuse-Response-Team der Freien Universität Berlin können helfen, den Schaden einzuschätzen und ggf. zu begrenzen. Informationen zum Security- und Abuse-Management der ZEDAT finden sich unter:

https://www.zedat.fu-berlin.de/AbuseManagement

Falls ein Angreifer Zugriff auf dienstliche Daten hatte, kann dann von den Kolleg:innen ggf. eine Mitteilung an den IT-Sicherheitsbeauftragen der Freien Universität oder den Datenschutzbeauftragen erfolgen.

Konten bei anderen Anbietern

Angreifer, die Zugriff auf das gesamte persönliche Postfach hatten, wissen dadurch ebenfalls, welche Konten ggf. bei externen Anbietern bestehen. Auch dort sollte also überprüft werden, ob es einen Einbruch gab und ggf. sicherheitshalber die Zugangsdaten geändert werden. Das Passwort des eigenen FU Accounts darf aber grundsätzlich an keiner anderen Stelle verwendet werden!

Wie kann ich zweifelsfrei echte E-Mails erkennen?

Absenderangaben sind bei E-Mails genauso leicht zu fälschen wie bei der herkömmlichen (Brief-) Post. Sowohl beim Layout als auch in der Wortwahl wird dabei eine möglichst perfekte Täuschung angestrebt. Ein gesundes Misstrauen im Umgang mit elektronischer Kommunikation ist daher unerlässlich.

Eine zuverlässige Überprüfung, ob eine Mail tatsächlich vom angeblichen Absender stammt, ist durch die Nutzung elektronischer Signaturen möglich. Angehörige der FU können sich bei Interesse ein sogenanntes Personenzertifikat, mit Hilfe dessen eigene E-Mails signiert werden können, bei der für sie zuständigen Stelle ihres Bereichs ausstellen lassen. Weitere Informationen dazu finden sich unter:

https://www.zedat.fu-berlin.de/Zertifikate