Erkennen von Spam- bzw. Phishing-E-Mails

05.10.2024 02:29:20

FAQ-Artikel-Ausdruck

Kategorie:	Anwenderbetreuung::Allgemein	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	15:13:41 - 28.06.2021

Schlüsselwörter

Sicherheit; E-Mail

Symptom (öffentlich)

Wie kann ich eine bösartige E-Mail erkennen?

Problem (öffentlich)

Lösung (öffentlich)

Erkennen von Spam- bzw. Phishing-E-Mails E-Mails mit schädlichem Code gefährden ggf. nicht nur Ihr eigenes IT-System bzw. Ihren eigenen Account, sondern auch weitere Personen und IT-Systeme. Öffnen Sie eine E-Mail nur dann, wenn Sie sicher sind, dass diese mit hoher Wahrscheinlichkeit ungefährlich ist. Mit den nachstehenden Kriterien können Sie beurteilen, ob eine E-Mail vertrauenswürdig ist.

Bei einer E-Mail kann sich schädlicher Code entweder im Anhang befinden oder in der E-Mail selbst, wenn diese im HTML-Format vorliegt. E-Mails im nur-Text-Format sind eher unkritisch, da dort kein Code hinterlegt ist.
Folgende grundsätzliche Fragen sollten Sie sich vor dem Öffnen einer E-Mail stellen:
- Ist die E-Mail - zunächst der Betreff, später der Inhalt - auf den ersten Blick seriös?

Offensichtlich unseriöse E-Mails sollten Sie nicht öffnen, sondern direkt löschen. Viele Spam-E-Mails können Sie über den bewusst allgemein gehaltenen Betreff erkenn, wenn dort z. B. nur "Ihre Rechnung", "Mahnung", oder "Dringende Nachricht" steht. Viele Rechtschreibfehler, seltsame Grammatik und falsche Darstellung von Umlauten sollten ebenfalls Skepsis hervorrufen.

- Stimmen Absendername und Absender-E-Mail-Adresse überein? Stimmen Links überein?

Wenn die Adressatendaten von E-Mail und Anschreiben nicht übereinstimmen, sollte das misstrauisch machen. Aber auch wenn diese übereinstimmen, ist das kein Freifahrtschein, da Adressaten einer E-Mail leicht gefälscht werden können. So können Sie z. B. Post von sich selbst oder von hochrangigen Persönlichkeiten erhalten.
Bei erhaltenen Links können Sie prüfen, ob der Link dahin führt, wohin der Text suggeriert: Fahren Sie mit der Maus über den Link (nicht anklicken!) und vergleichen, ob der aufpoppende Informationstext des Links dem Text der E-Mail entspricht. Der aufpoppende Informationstext zeigt, wohin der Link wirklich führt und nicht der Text der E-Mail.

- Ist die E-Mail an Sie persönlich adressiert oder allgemein gehalten?

Eine allgemein gehaltene Anrede deutet darauf hin, dass der Absender Sie nicht kennt. Das ist bei offiziellen E-Mails von Ihrer Bank, Ihrem Internetanbieter usw. eher unüblich und daher verdächtig. Aber auch eine direkte Anrede kann täuschen, wenn z. B. Ihre E-Mail-Daten öffentlich zugänglich sind oder ein Bekannter einen Virus hat, der sich an alle Kontakte in dessen Adressbuch selbst verschickt.

- Handelt es sich um eine HTML-E-Mail?

In HTML-E-Mails ist Code eingebettet, der für Formatierungen, Bilder, Schriftarten usw. zuständig ist. Allerdings kann dieser auch missbraucht werden und Skripte enthalten, die Dinge ausführen, die Sie nicht möchten (Schadsoftware installieren, Passwörter ausspähen, die Festplatte löschen usw.). Daher sind HTML-E-Mails grundsätzlich bedenklich. Deshalb sollten E-Mails vorzugsweise im nur-Text-Format geöffnet werden.

- Haben Sie einen Dateianhang erwartet?

Mit Dateianhängen verhält es sich wie mit Postpaketen im richtigen Leben: ohne Bestellung bzw. Absprache klingelt der Paketdienst nicht an der Tür und in diesem Fall kann es ja auch nicht für den Nachbarn sein. Also Vorsicht bei unerwarteten Dateianhängen.

- Wie lautet der Name des Anhangs? Welches Dateiformat hat der Anhang?

Manchmal deutet schon der Dateiname auf einen unseriösen Inhalt hin, z. B. wenn dort Worte auftauchen die neugierig machen (sollen), wie "dringend", "Hauptgewinn", "Geschenk" oder ähnliches. Ausführbare Dateien sind immer höchst verdächtig und sollten niemals direkt ausgeführt werden. Typische Endungen sind im Anschluss aufgelistet.
Achtung: Die Liste ist unvollständig. Außerdem gibt es noch weitere

Fallstricke:

- Für den Dateityp zählen nur die Zeichen nach dem letzten Punkt im Dateinamen. Zum Beispiel ist die Datei "Lottogewinne.pdf.exe" keine PDF-Datei, sondern eine EXE-Datei.
- Je nach Systemkonfiguration werden Dateiendungen unterdrückt, so dass die Datei "Rechnung.txt.exe" im Dateimanager als "Rechnung.txt" angezeigt werden kann und per Doppelklick ausgeführt wird.
- Der Dateityp kann durch viele Leerzeichen zwischen Dateinamen und Endung verschleiert bzw. je nach Ansicht im E-Mail-Programm anders wahrgenommen werden. Zum Beispiel: "Schokoladenkuchenrezept.pdf .exe"

Dateiendung	Beschreibung
.exe .com .bat	Ausführbare Dateien, die Schadcode enthalten können.
.msi .reg .sys	Ausführbare Systemdateien, die Schadcode enthalten können.
.vbs .js .ps .html	Programm-Scripte, die Schadcode enthalten können.
.doc .docx .xls .xlsx .odt .odp	Dokumente von Office-Programmen können Makros enthalten, die beim Aufrufen der Dateien ausgeführt werden.
.zip .rar	Gepackte Archiv-Dateien, die praktisch alles enthalten können.
.pdf	Plattformübergreifendes Dateiformat für die Anzeige von Dokumenten. PDF-Dateien können z. B. über JavaScript-Elemente auch Schadcode enthalten
.jpg .gif .bmp	Bilddateien, die theoretisch Schadcode enthalten können.
.mpg .avi .mov	Videodateien, die theoretisch Schadcode enthalten können.
.mp3 .wav	Audiodateien, die theoretisch Schadcode enthalten können.
.txt	Einfacher Text, der in der Regel ungefährlich ist.

- Ist der Anhang mit einem Virenscanner überprüft worden?

Prüfen Sie verdächtige Dateianhänge mit einem Virenscanner. Aber bedenken Sie dabei auch: Die Virenscanner helfen oft nur bei älteren und bekannten Viren.
Für Rückfragen stehen wir Ihen gerne unter it-sicherheit@phil-uni.goettingen.de zur Verfügung.