

Wir haben was gegen Phishing.

Retarus Anti- Phishing-Guide

Phishing-E-Mails, die es trotz E-Mail-Security bis in Ihr Postfach geschafft haben, haben noch einen starken Gegner: nämlich Sie.

Erfahren Sie, wie Sie sich zuhause und im Büro vor Online-Betrug schützen.



Seien Sie wachsam.

Rechnen Sie jederzeit mit Online-Betrugsversuchen. Die Wahrscheinlichkeit, dass Sie in eine Phishing-Falle tappen, sinkt dadurch enorm.

i Phishing ist eine Online-Betrugsform, bei der Cyberkriminelle versuchen, Schadprogramme zu verbreiten, Daten abzugreifen und sich finanzielle Vorteile zu verschaffen. Dabei arbeiten sie mit gefälschten Identitäten und manipulativen Botschaften, die typisch menschliche Eigenschaften wie Gutgläubigkeit, Hilfsbereitschaft oder Angst ausnutzen (Social Engineering).



Online-Betrüger tarnen sich gerne als gute Bekannte.

Online-Betrüger geben sich in Phishing-E-Mails als Freunde und Familienmitglieder aus, schlüpfen in die Rolle von Kollegen, Vorgesetzten oder Geschäftspartnern und sprechen Sie im Namen von offiziellen Institutionen, bekannten Finanzdienstleistern oder Online-Portalen (z. B. Ihre Bank, PayPal, Amazon, ...) an.



Das heißt: Auch wenn Sie den Absender einer E-Mail „kennen“, kann es sich um einen Phishing-Versuch handeln.

Die Phishing-Qualität steigt: technisch, inhaltlich, optisch.


Phishing-E-Mails mit ewig langen kryptischen Links und plumpen Handlungsanweisungen in schlechtem Deutsch und Design werden immer seltener. Die Phishing-Mails der neuen Generation sind technisch ausgeklügelt, perfekt formuliert und professionell gestaltet.



Gefälschte E-Mails, manipulierte Absender, Anhänge, Downloads und Webseiten wirken oft täuschend echt und sind selbst auf den zweiten Blick nicht unbedingt als Fälschungen zu erkennen.

Seien Sie zurückhaltend.

Wenn Sie das Gefühl haben, dass mit einer E-Mail oder mit einer Webseite etwas nicht stimmt, üben Sie sich in Zurückhaltung. Im Falle eines Phishing-Angriffs ist keine Reaktion die beste Verteidigung.

 Cyberkriminelle verpacken Schadprogramme (Malware) – die Ihren Computer und im schlechtesten Fall die gesamte IT-Infrastruktur lahmlegen – in E-Mail-Anhängen, hinter Links und Download-Optionen.



1 Klicken Sie in verdächtigen E-Mails niemals auf Links (auch nicht auf Abmelde-Links*).

2 Öffnen/laden Sie in verdächtigen E-Mails keine Anhänge (Malware).

3 Antworten Sie nicht auf verdächtige E-Mails*, leiten Sie die E-Mails nicht weiter.

4 Geben Sie auf verdächtigen Webseiten niemals Benutzernamen, Passwörter oder andere persönliche Daten ein.

*damit würden Sie nur Ihre E-Mail-Adresse bestätigen

Achtung, Chefmasche (CxO Fraud)!

CxO Fraud ist eine besonders dreiste Phishing-Methode, bei der Cyberkriminelle sich als Führungskraft ausgeben und Mitarbeiter unter Vortäuschung falscher Tatsachen (z. B. Notfallsituation) zu Handlungen drängen (z. B. Geld anweisen, vertrauliche Informationen preisgeben).

Typisch für Phishing-Mails dieser Art: die hohe Dringlichkeit und die Bitte um vertrauliche Behandlung.

Sie kennen den Absender einer E-Mail mit fragwürdigem Inhalt?

Überprüfen Sie die Echtheit der E-Mail durch ein persönliches Gespräch/Telefonat mit dem Absender.

Sie glauben, dass Sie in eine Phishing-Falle getappt sind?

Zögern Sie keine Sekunde, Ihren Vorgesetzten und/oder die Kollegen in der IT zu informieren. Diese wissen, was zu tun ist.

Seien Sie misstrauisch.

Online-Betrüger lieben alles, was Menschen bewegt und beschäftigt. Zu Themen, die uns persönlich (be)treffen, die intensiv von den Medien bespielt werden, die uns mit Sorge oder Freude erfüllen, gibt es deshalb oft auch den „passenden“ Phishing-Köder.



Nicht nur online! Betrüger sind nicht nur per E-Mail und auf Webseiten unterwegs, sondern auch in den Sozialen Medien, per SMS, am Telefon und sogar an der Tür.



Seien Sie misstrauisch, wenn ein Angebot „wie gerufen“ kommt, wenn eine Nachricht sie irgendwie triggert und wenn es um Anweisungen mit Homeoffice-Bezug geht. Nehmen Sie sich am besten kurz Zeit und beobachten Sie die Gedanken und Gefühle, die eine Botschaft bei Ihnen auslöst. „Leitet“ Sie eine Routine, ein Prinzip, eine allgemeine Regel? „Spricht“ eine Autorität? Schwingt eine Angst mit? Winkt eine allzu perfekte Gelegenheit? Falls ja: Tief durchatmen, noch mal nachdenken, evtl. recherchieren – und erst dann reagieren. Oder eben nicht.

Mit welchen Tricks Cyberkriminelle versuchen, Malware zu verbreiten, Daten abzugreifen, Geld zu verdienen:

Offizielle, unverzichtbare oder exklusive Informationen als Newsletter-Abo, im E-Mail-Anhang oder zum Herunterladen

Einmalige Gelegenheiten wie z. B. Angebote zu stark nachgefragten oder zeitlich begrenzt verfügbaren Produkten, hohe Gewinnchancen, clevere Anlagetipps, ...

Datenabfrage/Datenabgleich von **Online-Accounts** (Mitarbeiter, Kunde, User, Member, Patient, ...)

Handlungsanweisungen und Bitten, die **mit „Druck“** arbeiten (z. B. Notlage, Versäumnis, Gefahr, ...)

Download oder Installation von Software oder Sicherheitsupdates

Passwortabfrage für die Teilnahme an einer Videokonferenz

Datenabfrage/Datenabgleich für die Freischaltung eines **Remote-Tools** (Fernwartung)

Sie zweifeln an einer IT-Anweisung in Bezug auf Ihre Arbeit im Homeoffice?
Fragen Sie lieber einmal zu oft bei den Kollegen in der IT nach.

Das einzig Wahre gegen Phishing: Eine gute E-Mail-Security und Sie!

Seien Sie **wachsam**, rechnen Sie mit Online-Betrugsversuchen. Seien Sie **zurückhaltend**, vermeiden Sie spontane Klicks und Downloads. Seien Sie **misstrauisch**, hinterfragen Sie Botschaften, nutzen Sie Ihren gesunden Menschenverstand und mehr als eine Informationsquelle.

Retarus Email Security

Damit E-Mail im Unternehmen läuft und nicht bremst.

retarus.de/email-security

