Internetrecht-Ratgeber

Phishing: So reagieren Sie auf verdächtige E-Mails

Schädliche Phishing-Mails: Wie Sie die betrügerischen Mails und SMS erkennen können und wie Sie sich verhalten sollten – zu Hause und unterwegs.

13. Juni 2024 • 7 Minuten Lesezeit

Artikel teilen

Inhaltsverzeichnis

Auf den Punkt

- Mit Phishing-Mails versuchen Cyberkriminelle, an persönliche und finanzielle Informationen wie Passwörter und Kontodaten kommen.
- Typische Hinweise auf Phishing sind gefälschte Absenderadressen, Dringlichkeitsappelle und Rechtschreibfehler. Allerdings wird Phishing immer raffinierter und damit schwerer zu erkennen.
- Opfer von Phishing sollten sofort alle Passwörter ändern, betroffene Konten sperren und Anzeige erstatten.
- Tätern drohen Geld- und Freiheitsstrafen bis zu fünf, in schweren Fällen bis zu zehn Jahren.

Was sind Phishing-Mails?

Jeder, der viel im Internet unterwegs ist, wird bereits festgestellt haben, dass die Fantasie der Cyberkriminellen keine Grenzen kennt. Abofallen, Fake-Shops, Love-Scams, Job-Scamming, Identitätsdiebstahl, Cyberangriffe und viele andere Betrugsmaschen machen die digitale Welt unsicher. Eine der häufigsten und zugleich gefährlichsten Bedrohungen sind Phishing-Mails.

Phishing ist eine Methode, bei der Betrüger versuchen, durch gefälschte E-Mails an persönliche Informationen wie Passwörter, Kreditkartendaten oder wichtige Zugangsdaten zu gelangen. Diese E-Mails können sehr überzeugend wirken und manchmal ist es gar nicht so einfach, sie auf den ersten Blick zu erkennen.

Wie eine klassische Phishing-Mail aussieht? Ungefähr so:

Betreff:
Dringendes Sicherheitsupdate erforderlich!

Von:
Kundenservice (support@examplebank.com)

Nachricht:
Sehr geehrte/r [Name des Empfängers],

wir haben ungewöhnliche Aktivitäten in Ihrem Konto festgestellt und benötigen Ihre sofortige Aufmerksamkeit, um Ihr Konto zu schützen. Aus Sicherheitsgründen wurde Ihr Konto vorübergehend gesperrt, bis die Angelegenheit geklärt ist.

Um Ihr Konto wieder zu aktivieren und die Sicherheit zu bestätigen, klicken Sie bitte auf den untenstehenden Link und folgen Sie den Anweisungen zur Verifizierung Ihrer Identität:
[Link zur vermeintlichen Bank-Website]

Bitte beachten Sie, dass, wenn Sie innerhalb von 24 Stunden nicht reagieren, Ihr Konto dauerhaft gesperrt bleiben könnte.

Vielen Dank für Ihre schnelle Reaktion auf diese dringende Angelegenheit.

Mit freundlichen Grüßen, Ihr Kundenservice-Team

Wenn Sie nun auf den angegebenen Link klicken, gelangen Sie zu einer gefälschten Website, die täuschend echt aussieht. Schon hat der Phisher Sie auf dem Haken: Sie verraten Ihre persönlichen Daten wie Benutzernamen, Passwörter, Kontodaten und Kreditkarteninformationen.

Die Kriminellen nutzen aber auch gern aktuelle Anlässe für ihre E-Mail-Betrugsmasche. So gab es beispielsweise während der Corona-Pandemie eine Flut von Phishing-E-Mails, welche vorgaben, von Gesundheitsorganisationen zu stammen und wichtige Maßnahmen zum Virus zu enthalten. Naturkatastrophen, wie Überschwemmungen oder Erdbeben, nutzen die Cyberbetrüger ebenfalls aus: Sie setzen auf die Solidarität und das Mitgefühl der Menschen, um Spendenbetrug zu begehen. Sie versenden E-Mails mit der Bitte um finanzielle Unterstützung für die Opfer, leiten die Gelder jedoch auf betrügerische Konten um.

Das sagt die Statistik: Phishing-Angriffe nehmen zu

Das Bundeskriminalamt hat für das Jahr 2023 in Deutschland 134.407 Fälle von Cybercrime (Computerbetrug, Ausspähen und Abfangen von Daten, Fälschung beweiserheblicher Daten, Datenveränderung etc.) registriert. 2013 waren es noch 64.426 Fälle, was einer Steigerung von [illegible] Vorfälle in diesem Bereich nicht angezeigt werden, stellen diese Zahle[illegible] Kriminalitätsrate dar.

Dabei nehmen Phishing-Angriffe nicht nur von Jahr zu Jahr zu, sondern werden auch immer raffinierter. Früher konnte man Phishing leicht an fehlerhaften Formulierungen erkennen, was auf den ersten Blick auffiel. Inzwischen sind die Angriffe subtiler geworden und die Ansprache ist häufig grammatikalisch korrekt. Mit dem Aufkommen von KI-Technologien dürften die Betrugsmaschen noch ausgeklügelter und schwerer zu identifizieren werden.

Von Whaling bis Vishing: Diese Phishing-Maschen gibt es

Neben der klassischen Phishing-Mail gibt es noch weitere Phishing-Methoden:

- Smishing (SMS-Phishing / Whatsapp-Phishing)
- Vishing (Voice Phishing)
- Spear-Phishing
- Whaling

Was ist Smishing?

Der Begriff "Smishing" ist eine Kombination aus "SMS" und "Phishing". Bei dieser Betrugsmasche nutzen die Kriminellen SMS- oder WhatsApp-Nachrichten, um persönliche und finanzielle Daten von Opfern zu erschleichen. Bei einem Smishing-Angriff erhalten die Betroffenen eine Nachricht, welche sie beispielsweise darüber informiert, dass es ein Problem mit ihrem Bankkonto gibt oder sie eine wichtige Lieferung verpassen werden. Die Nachricht enthält einen Link, der, wenn angeklickt, die Opfer auf eine gefälschte Website führt, wo sie persönliche Daten eingeben sollen.

Aktuell! Fake-SMS Paketbenachrichtigungen: Nur nicht anklicken!

Derzeit verschicken Cyberkriminelle verstärkt gefälschte Paketbenachrichtigungen per SMS, um Schadsoftware zu platzieren oder an Ihre persönlichen Daten zu gelangen.

Das Ganze nennt sich „Smishing“ aus SMS und Phishing. Gerade in Zeiten, in denen der Online-Handel boomt, sind Opfer leicht gefunden. In der SMS werden die Empfänger darauf hingewiesen, dass ihr Paket oder Geschenk verschickt wurde und sie die Sendung per Link überprüfen und bestätigen sollen.

Doch seien Sie vorsichtig! Mit einem Klick auf den Link wird die gefährliche Schadsoftware FluBot auf Ihrem Handy installiert und kann dann auf alle persönlichen Daten zugreifen. So können z. T. teure SMS in die Welt verschickt werden, ohne dass Sie es bemerken. Zudem hat es die Schad-App auf Daten abgesehen, die bei Banking-Apps eingegeben werden.

Laut Polizeibehörden sind vor allem Nutzer von Android-Handys betroffen. Wer bereits auf den Link geklickt hat, sollte in Form von Screenshots möglichst viele Beweise sammeln und mit dem Smartphone möglichst schnell zur nächsten Polizeidienststelle gehen, um Anzeige zu erstatten.

Erst anschließend sollten Sie die SMS löschen, die Rufnummer des Absenders blockieren und eine Drittanbietersperre beim Mobilfunkanbieter einrichten, um teure Folgekosten zu vermeiden.

Als letzten Schritt empfehlen die Experten, alle persönlichen Daten in der Cloud oder auf einer Speicherkarte zu sichern und im abgesicherten Modus nach unbekannten und nicht selbst installierten Apps zu suchen und diese zu entfernen. Danach muss das Handy allerdings neu gestartet oder gar zurückgesetzt werden.

Vishing: Verdächtige Anrufe

Vishing steht für "Voice Phishing". Bei dieser Betrugsmasche nutzen Kriminelle Telefonanrufe anstelle von E-Mails oder Textnachrichten. Dabei machen sie sich die menschliche Neigung zunutze, Sprachkommunikation als vertrauenswürdiger einzustufen. So fällt es den Betrügern oft leichter, am Telefon Überzeugungsarbeit zu leisten. Sie geben sich als seriöse Institutionen wie Banken, Kreditkartenunternehmen oder sogar Behörden aus und behaupten, es gäbe ein dringendes Problem mit dem Konto oder der persönlichen Sicherheit des Opfers. Es folgt ein „Datenabgleich“ oder ein „Datenupdate“, bei dem wiederum sensible Daten preisgegeben werden.

Datenklau durch Spear-Phishing und Whaling

„Spear-Phishing“ und „Whaling“ bedeuten auf Deutsch „Speerfischen“ und „Walfang“. Die große Angel-Metapher wurde gewählt, um die Art und Weise zu beschreiben, wie Betrüger versuchen, ihre Opfer anzulocken und zu fangen.

Beim Spear-Phishing werden ausgewählte Personen oder Organisationen wie Behörden und Vereine gezielt angegriffen – wie bei einer Jagd mit dem Speer. Beim Whaling haben es die Kriminellen auf besonders große Fische abgesehen, also auf hochrangige Ziele wie Geschäftsführer und leitende Angestellte. Beide Phishing-Methoden sind äußerst sorgfältig konstruiert und können sogar aktuelle oder sehr spezifische Informationen enthalten, die aus öffentlich zugänglichen oder illegal erworbenen Quellen stammen. Dadurch wirken diese Phishing-Mails besonders authentisch.

Anzeichen von Phishing erkennen

Auch wenn Phishing-Mails immer raffinierter werden, so gibt es doch eine Reihe von Merkmalen, die Hinweise auf ihren betrügerischen Charakter geben. Oft verwenden Phishing-Mails Adressen, die denen offizieller Organisationen ähneln, aber **kleine Fehler oder Tippfehler** aufweisen. Beispielsweise könnte „support@bank.com“ als „suport@bank.com“ fehlgeschrieben sein.

Des Weiteren nutzen Phishing-E-Mails häufig Sprache, die ein Gefühl der **Dringlichkeit oder Angst erzeugt**. Formulierungen wie „Sofortiges Handeln erforderlich“ oder „Ihr Konto wird gesperrt“ sind typisch und sollen Sie zu vorschnellen Handlungen drängen. Solche Nachrichten enthalten oft auch **Grammatik- und Rechtschreibfehler**, die ein weiteres Warnsignal darstellen. Während manche Betrugsversuche sehr ausgeklügelt sind, weisen viele aufgrund schlechter Übersetzungen oder hastiger Zusammenstellung Mängel auf.

Ein weiteres häufiges Merkmal von Phishing-Mails ist die **Aufforderung, persönliche oder finanzielle Informationen preiszugeben**. Keine seriöse Organisation würde solche sensiblen Daten über eine unsichere Plattform wie E-Mail erfragen. Auch **verdächtige Links** oder die Aufforderung, **Anhänge** zu öffnen, sind alarmierende Zeichen. Bevor Sie auf einen Link klicken: Bewegen Sie den Mauszeiger über den Link, denn so können Sie die tatsächliche URL sehen. Die **unpersönliche Anrede**, wie „Sehr geehrter Kunde“ oder „Liebe Nutzerin, lieber Nutzer“, ist ebenfalls typisch für solche Massennachrichten.

Zudem sollten Sie skeptisch sein bei Angeboten, die zu gut klingen, um wahr zu sein, wie das **Versprechen großer Geldgewinne** oder extrem günstiger Angebote. Schließlich ist auch eine ungewöhnliche oder **unprofessionell wirkende Gestaltung** der E-Mail meistens ein Indikator für Phishing.

Schutz vor Phishing: Das können Verbraucher tun

Ihr Schutz zu Hause

- Halten Sie Ihre Antiviren-Software stets aktuell und pflegen Sie Ihre Browser-Software regelmäßig mit aktuellen Sicherheits-Updates.
- Übernehmen Sie die Internetadresse Ihrer Bank nicht aus Links; tippen Sie sie lieber selbst ein.
- Nutzen Sie beim Eingeben von vertraulichen Daten nur verschlüsselte Verbindungen. Sie erkennen diese an dem Buchstaben "s" im „https“ einer Internetadresse (URL) und dem Symbol eines Vorhängeschlosses auf der Browser-Statuszeile.
- Überprüfen Sie das Sicherheitszertifikat der Website, indem Sie auf das Schlosssymbol in der Statuszeile doppelklicken. Im Dialogfenster können Sie beispielsweise prüfen, ob der im Sicherheitszertifikat angegebene Domainname mit dem Namen der von Ihnen angeforderten Webseite übereinstimmt.
- Kommt Ihnen eine Mail einer Ihnen bekannten Adresse auffällig vor, öffnen Sie diese nicht, sondern verifizieren Sie sie durch eine kurze telefonische Anfrage.
- Geben Sie niemals Passwörter, PIN oder TAN heraus. Banken oder seriöse Unternehmen würden Sie niemals per Mail oder Telefon dazu auffordern.
- Kontrollieren Sie Ihr Konto regelmäßig.
- Checken Sie, ob Ihr Geldinstitut dem Sperr-Notruf 116 116 angeschlossen ist, denn dann können Sie schnell und kostenlos Kreditkarten sperren lassen und den Onlinebanking-Account deaktivieren. Den Notruf nehmen Sie am besten gleich in Ihr Handy-Telefonverzeichnis auf.

Ihr Schutz unterwegs, am Hotspot und im Hotel

- Fragen Sie den Betreiber nach Sicherheitsvorkehrungen. Lassen Sie sich im Café oder Hotel die korrekte WLAN-Kennung nennen und wählen diese manuell aus.
- Schließen Sie eigene USB-Sticks oder externe Festplatten nur dann an, wenn der Hotel-PC über ein aktuelles Virenschutzprogramm verfügt.

- Deaktivieren Sie in Ihrem Smartphone oder Laptop die automatische Verbindung mit jedem öffentlichen Netzwerk, das nicht durch ein Kennwort geschützt ist.
- Deaktivieren Sie in den Netzwerkeinstellungen Ihres Betriebssystems die Dateifreigabe.
- Geben Sie Anmeldedaten im öffentlichen Raum diskret ein. Nützlich können spezielle Schutzfolien sein, die Ihr Display vor neugierigen Blicken Unbefugter abschirmen.

Was ein gutes Passwort ausmacht

Sensible Daten brauchen im Netz einen besonderen Schutz. Denn mit ausgespähten Passwörtern können Unbefugte Ihre E-Mails lesen, in Ihrem Namen einkaufen oder Gerüchte in die Welt setzen. Damit Sie weiterhin auf der sicheren Seite sind, haben wir Ihnen Tipps für gute Passwörter zusammengestellt.

- Kein Passwort für alle Fälle. Wenn ein Zugang geknackt ist, sind alle anderen inklusive Online-Banking auch nicht mehr sicher. Verschiedene Zugänge sollten also auch verschiedene Passwörter haben.
- Ein gutes Passwort besteht aus mindestens acht Zeichen. Es enthält Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen – am besten eine wie zufällig wirkende Kombination.
- Ungeeignet sind Geburtsdaten, Namen aus Ihrer Familie, Zahlenfolgen wie 123456 – und das Wort Passwort.
- Passwörter sollten alle sechs bis acht Wochen gewechselt werden.

Auf Phishing-Mail reingefallen – was tun?

Normalerweise gehen Sie verantwortungsvoll mit Ihren Daten um, aber dennoch ist es passiert: Sie sind auf einen Betrüger hereingefallen. Jetzt ist **Eile geboten**. Wenn Sie auf einer gefälschten Bank-Seite Ihre Daten eingegeben haben, melden Sie sich bei Ihrer Bank und lassen das **Konto sperren**. Melden Sie die Phishing-Mail dem Unternehmen, als das sich der Betrüger ausgegeben hat.

Erstatten Sie **Strafanzeige** bei der Polizei. Wer sich unbefugt Zugang zu besonders gesicherten Daten verschafft, macht sich strafbar. Und melden Sie den Vorfall möglichst auch einer **Verbraucherzentrale**. Diese haben ein wachsames Auge auf Phishing-Angriffe und können andere Internet-User warnen.

Ändern Sie sofort alle wichtigen Passwörter und PINs für Ihre Bankkonten, E-Mail-Konten, soziale Netzwerke und andere Online-Dienste. Außerdem sollten Sie einen vollständigen Scan Ihres Computers und Smartphones mit zuverlässigen **Antivirus-Programmen** durchführen. So können Sie Malware oder Spyware aufdecken. Und aktivieren Sie, wo möglich, die Zwei-Faktor-Authentifizierung, falls noch nicht geschehen.

DHL Fake-SMS geöffnet – was tun?

Wenn Sie die SMS nur öffnen, passiert nichts. Problematisch wird es, wenn Sie auf den Link in der SMS geklickt und sensible Daten eingegeben haben. Dann gilt das gleiche Vorgehen wie bei der Phishing-Mail. Hier noch einmal die Handlungsschritte im Überblick:

Fake-SMS geöffnet – was tun?

- Keine Links anklicken, keinen Anweisungen folgen
- Falls Link angeklickt und Daten eingegeben, sofort Bank kontaktieren und Konto sperren
- Echtes Dienstleisterunternehmen benachrichtigen (z.B. DHL)
- Anzeige bei der Polizei erstatten
- Verbraucherzentrale melden
- Passwörter ändern und Antivirus-Programm anschmeißen

Manchmal werden heimlich Programme auf dem Smartphone installiert, wenn Sie beispielsweise auf einen Link geklickt und etwas heruntergeladen haben. Suchen Sie die versteckte App und deinstallieren Sie diese. Falls das nicht klappt,

Starten Sie Ihr Smartphone im abgesicherten Modus neu. Wenn auch das nicht hilft, setzen Sie Ihr Handy auf die Werkseinstellungen zurück.

Betrügerische E-Mails: Diese Strafen drohen den Tätern

Phishing fällt unter den **Tatbestand des Betrugs** nach § 263 StGB und kann mit Freiheitsstrafen bis zu fünf Jahren oder mit Geldstrafen geahndet werden. In schweren Fällen, etwa bei gewerbsmäßigem Betrug, kann die Freiheitsstrafe zwischen sechs Monaten und zehn Jahren liegen.

Wenn Phishing eingesetzt wird, um sich unbefugt Zugang zu Daten zu verschaffen, die nicht für den Täter bestimmt und gegen unbefugten Zugriff besonders gesichert sind, greift der „**Hackerparagraph**“ 202a StGB (Ausspähen von Daten). Hier drohen Geldstrafen oder Freiheitsstrafen bis zu drei Jahren. Werden Daten verändert, gelöscht oder unbrauchbar gemacht, kann dies unter § 303a StGB (**Datenveränderung**) fallen. Auch hier sind Freiheitsstrafen bis zu zwei Jahren oder Geldstrafen möglich.

Liegt ein **Identitätsdiebstahl** durch Phishing vor, bei dem die Betrüger Ihre Daten verwenden, um in Ihrem Namen zu handeln, so kann § 269 StGB Fälschung beweiserheblicher Daten und § 270 StGB Täuschung im Rechtsverkehr bei der Datenverarbeitung vorliegen. Diese Paragraphen kommen zur Anwendung, wenn gefälschte Dokumente oder digitale Daten zur Täuschung im Rechtsverkehr verwendet werden. Es drohen Geldstrafen oder Freiheitsstrafen bis zu fünf Jahren.

Ähnliche Artikel zum Thema

Alle Artikel →

Urheberrechtsverletzung & Urheberrecht | Expertenrat der ARAG

Lesezeit 8 Minuten

Wer haftet für illegale Downloads?

Cybermobbing – was tun? | ARAG hilft

Lesezeit 7 Minuten

Schaden melden

Services