

Erkennen Sie Phishing? (#234)

Der folgende Wochentipp ist aus der kostenlosen App **Senioren mit Smartphone - Einfach erklärt** von Jonah Hadt. Möchten Sie weitere Tipps rund um das  Smartphone erhalten? Laden Sie sich gerne die kostenlose App herunter. (Verfügbar für Android, Apple und Windows)



Willkommen zum Tipp der Woche. **Jeden Sonntag um 12 Uhr** bietet die App „Senioren mit Smartphone“ neue Tipps zu Smartphone und Internet für Senioren und Technikinteressierte.

Glauben Sie, dass Sie Phishing gut erkennen können? Ich denke ich habe schon oft über Phishing oder E-Mail-Angriffe bei Senioren mit Smartphones gesprochen. Ich habe auch manchmal ein paar Beispiele gegeben, aber ich habe vor kurzem ein sehr gutes Projekt vom KIT (Karlsruher Institut für Technik) gefunden, wo man sich direkt testen lassen kann.

Die folgenden Punkte sollten immer beachtet werden, wenn es um Phishing geht:

1. Absenderadresse prüfen: Schauen Sie genau auf die E-Mail-Adresse des Absenders. Oft verwenden Betrüger Adressen, die echt aussehen, aber kleine Fehler enthalten.
2. Vorsicht bei dringenden Aufforderungen: Seien Sie misstrauisch bei E-Mails, die Sie zu schnellem Handeln drängen, wie „Ihr Konto wird gesperrt, wenn Sie nicht sofort handeln!“.
3. Persönliche Anrede fehlt: Seriöse Unternehmen sprechen Sie meist mit Namen an. Allgemeine Anreden wie „Sehr geehrter Kunde“ können ein Warnzeichen sein.

4. Rechtschreib- und Grammatikfehler: Achten Sie auf auffällige Sprachfehler. Seriöse Unternehmen machen selten solche Fehler.
5. Links überprüfen: Fahren Sie mit der Maus über einen Link (ohne zu klicken). Am unteren Bildschirmrand sehen Sie dann die tatsächliche Zieladresse. Auf dem Handy können Sie den Link länger gedrückt halten, um die Vorschau zu sehen.
6. Vorsicht bei Dateianhängen: Besonders vorsichtig sollten Sie bei Dateianhängen sein. Achten Sie auf die Dateiendung – das ist der Teil nach dem letzten Punkt im Dateinamen. Gefährliche Endungen sind z.B. .exe, .bat, oder .scr. Diese können Schadprogramme enthalten.
7. Unerwartete Anhänge: Öffnen Sie keine Anhänge, die Sie nicht erwartet haben, selbst wenn sie harmlos erscheinen.
8. Vertrauliche Informationen: Geben Sie niemals vertrauliche Daten wie Passwörter oder Bankdaten per E-Mail weiter. Seriöse Unternehmen fragen solche Informationen nicht per E-Mail ab.
9. Im Zweifel nachfragen: Wenn Sie unsicher sind, kontaktieren Sie das Unternehmen direkt über die offizielle Webseite oder Telefonnummer – nicht über Kontaktdaten aus der verdächtigen E-Mail.

Zum Testen klicken Sie einfach hier: <https://nophish-quiz.secuso.org/>

Sie sehen nun immer die fast identische E-Mail von „Mein Paket Service“. Sie haben dort ein Paket bestellt und erhalten nun eine E-Mail von diesem Shop. Es könnte sich um einen Betrug handeln. Das KIT schreibt: „Sie sehen 9 E-Mails, die ähnlich wie die unten abgebildete aussehen. Entscheiden Sie jeweils, ob es sich um eine vertrauenswürdige E-Mail handelt oder nicht. Stellen Sie sich vor, Sie erwarten ein wichtiges Paket und gehen Sie davon aus, dass Ihr Name „Max Müller“ und Ihre E-Mail-Adresse „max.mueller.1973@web.de“ ist. Schauen Sie sich die Fallbeispiele immer genau an und entscheiden Sie mit den blauen Schaltflächen unten, ob es sich um Betrug handelt oder nicht. Das Ergebnis wird immer direkt nach der Beantwortung der Fragen angezeigt.“

TIPP: Wenn Sie das Quiz am Handy machen lohnt es sich das Handy einmal zu drehen damit man die E-Mail besser sehen kann.

Ist dies eine Phishing-E-Mail?

ein-paketservice.de <versand@mein-paketservice.de> 

Bestellung Ihrer Bestellung

Max Müller <max.mueller.1973@web.de>

ein  Paketservice [Mein Konto](#) | [mein-paketsei](#)

Hallo,

Bestellungsproblem für Dich, wichtig, dass wenn direkt re
nst Schaden.
behalten wenn [Click-here](#)

in Freund

ist eine automatisch versendete Nachricht. Bitte antworten Sie nicht auf dieses E-Mail, da die Adresse nur zur Versendung
richtig ist.

Ja

Nein

Am Ende des Quiz gibt es auch zwei sehr schöne Videos. Diese erklären einige Punkte noch einmal sehr gut. Schauen Sie sich gerne noch einmal an.

Teilen Sie mir gerne mit, ob Sie den Phishing-Test besser oder schlechter beantworten konnten als erwartet. Bleiben Sie sicher im Internet!

Hat Ihnen der Wochentipp gefallen?

Ich würde mich sehr freuen, wenn Sie uns bei unserem Projekt unterstützen würden. Jede Spende, egal wie groß oder klein, hilft mir, unsere Serverlaufzeiten aufrechtzuerhalten und die Kosten für den Betrieb des Projekts zu decken. Wenn Sie mir helfen möchten, können Sie gerne auf das folgende Konto spenden:

IBAN: DE33 1001 1001 2226 6677 82

BIC: NTSBDEB1XXX,

Inhaber: Jonah Hadt

Oder per PayPal [hier klicken](#).

Ansonsten unterstützen Sie die App sehr, mit einer 5-Sterne-Bewertung im Google Play Store. [Das können Sie hier tun](#).

Vielen vielen Dank!

Mehr Informationen / Fragen zu dem Thema?

Schicken Sie einfach eine E-Mail an app@jonahhadtd.de oder treten Sie der WhatsApp-Gruppe „Senioren mit Smartphone“ ([hier klicken](#)) oder der Signal-Gruppe ([hier klicken](#)) bei. Ich würde mich auch sehr über eine 5-Sterne-Bewertung im Google Play Store freuen, damit Sie das Projekt kostenlos unterstützen können ([hier klicken](#)). Herzlichen Dank dafür! Vielen Dank an alle!

Bis nächste Woche und viel Spaß mit den neuen Möglichkeiten. **Der nächste Tipp der Woche erscheint am kommenden Sonntag, den 14.07.24** um 12 Uhr. Bleiben Sie gesund und mit freundlichen Grüßen Jonah.

Das war der Wochentipp aus der kostenlosen App **Senioren mit Smartphone - Einfach erklärt** von Jonah Hadt. Möchten Sie weitere Tipps rund um  Smartphone erhalten. Laden Sie sich gerne die kostenlose App herunter. (Verfügbar für Android, Apple und Windows).