sosafe

INFOSHEET

Was ist der Unterschied zwischen Phishing & Spam?

Beides landet regelmäßig im Postfach. Doch was ist eigentlich der grundlegende Unterschied zwischen Spam und Phishing? Erfahren Sie, warum selbst bei vermeintlich ungefährlichen E-Mails Vorsicht geboten ist, und wie Sie sich vor Phishing und Spam schützen.

Phishing vs. Spam
– Was ist was?

	Spam	Phishing
Bedeutung	Spam ist auch als „Junk-Mail“ bekannt. Dabei handelt es sich um unerwünschte Werbe-Mails, die massenhaft versendet werden	Bei der Online-Betrugsmasche versuchen Cyberkriminelle sensible Informationen zu „angeln“ (engl. „to fish“).
Zahlen und Fakten	Bei 60 bis 90 Prozent aller versendeten Mails handelt es sich mittlerweile um Junk-Mail.	Im Durchschnitt fällt mehr als jede dritte Person auf Phishing-Mails herein.
Absichten / Ziele	Grundsätzlich hat Spam kommerzielle Absichten – will also für ein Produkt oder einen Service werben. Doch aufgepasst: Viele vermeintlich harmlose Spam-Mails entpuppen sich als Wolf im Schafspelz, bei denen es sich um Phishing-Mails mit gefährlichen Links oder Anhängen handelt.	Phishing-Mails sind darauf ausgerichtet, Bankdaten, Passwörter, Anmeldedaten oder ähnlich sensible Daten offenzulegen. Sie verfolgen immer boshafte Absichten und sollen den Opfern finanziell oder persönlich schaden.

Fun Fact “Spam”: Die Abkürzung Spam stand ursprünglich für „spiced pork and ham” (dt. „gewürztes Schweinefleisch und Schinken”). In einem Monty-Python-Sketch wurde in einem Restaurant dutzendweise Spam serviert – so oft, bis niemand mehr das Wort Spam hören wollte. Online wurde der Begriff umgedeutet und wird mittlerweile als Akronym für “send phenomenal amounts of mail”, also den massenhaften Versand von E-Mails, verwendet.

sosafe

www.sosafe.de

Checkliste

sosafe

www.sosafe.de

Woran erkenne ich gefährliche E-Mails?

Gefährliche E-Mails sind immer schwieriger zu erkennen, doch einige grundlegende Merkmale helfen Ihnen dabei. Seien Sie besonders vorsichtig, wenn ...

- ✓ E-Mails von unvollständigen Mail-Adressen stammen,
- ✓ sich falsch geschriebene Wörter häufen,
- ✓ Sie zu Handlungen aufgefordert werden
  (z. B. Ändern Sie Ihr Passwort innerhalb der nächsten Stunde),
- ✓ Ihnen die URL im E-Mail-Text merkwürdig vorkommt,
- ✓ Sie den Absender nicht kennen,
- ✓ Sie aufgefordert werden, Links oder Anhänge zu öffnen.

Sie haben eine potenzielle Phishing-Mail entdeckt? Dann klicken Sie so schnell wie möglich auf den Phishing Report Button, bevor Sie die E-Mail löschen.

Auf unserem Awareness-Blog mehr über Phishing und Co. erfahren