

Was tun, wenn eine verdächtige E-Mail in Ihrem Posteingang landet?

Der Umgang mit verdächtigen E-Mails gehört zum Grundwissen, mit dem Sie zum Schutz Ihrer Organisation vor Cyberkriminellen beitragen können. Wenn Sie nicht wissen, was bei Empfang einer verdächtigen E-Mail zu tun ist, fallen Sie vielleicht einem Phishing-Angriff zum Opfer.

Wir haben für Sie einige Tipps zusammengestellt:

E-Mail nicht beantworten

Wenn Sie eine verdächtige E-Mail erhalten, die von einer Ihnen bekannten Person zu stammen scheint, lassen Sie sich nicht dazu verleiten, aus Neugier auf diese E-Mail zu antworten. Dadurch erhöht sich womöglich das Sicherheitsrisiko. Wenn ein E-Mail-Konto kompromittiert wurde, ist der wahre Absender wahrscheinlich nicht die Person, die Sie kennen, sondern ein:e Cyberkriminelle:r.

E-Mail nicht weiterleiten

Halten Sie sich am besten an Folgendes: nicht auf unverlangte Links klicken und unverlangte Anhänge nicht öffnen. Wenn Sie doch einmal auf eine Phishing-E-Mail hereinfallen und auf einen schädlichen Link klicken oder einen schädlichen Anhang öffnen, werden möglicherweise unerwünschte Aktionen ausgeführt. Ein Beispiel: Sie öffnen ein verdächtiges, an eine E-Mail angehängtes Bild – anstelle des Bildes wird jedoch ein Installationsfenster geöffnet. Ein anderes Beispiel: Sie klicken auf einen schädlichen Link, der zu einer gefälschten Anmeldeseite führt.

Möglicherweise möchten Sie einen Link oder Anhang, der Ihnen verdächtig vorkommt, an eine Kollegin oder einen Kollegen weiterleiten, um nach Rat zu fragen. Tun Sie das nicht. Das Weiterleiten der E-Mail kann das Risiko erhöhen. Wenn Sie auf einen Link klicken oder einen Anhang öffnen und eine unerwartete Aktion ausgeführt wird, liegt ein eindeutiges Warnsignal vor. Leiten Sie ungewöhnliche oder verdächtige E-Mails nicht an andere Personen weiter. Dadurch erhöht sich das Risiko eines Sicherheitsvorfalls. Denn möglicherweise klicken Ihre Kolleg:innen ebenfalls auf den Phishing-Link.

E-Mail nicht als Spam markieren

Eine Spam-E-Mail enthält in der Regel unerwünschte Werbung. Spam-E-Mails sind zwar nervtötend, jedoch für gewöhnlich harmlos. Eine Phishing-E-Mail mit schädlichem Inhalt hingegen soll den Anschein erwecken, dass sie „echt“ ist. Phishing-E-Mails enthalten in der Regel eine Handlungsaufforderung (neudeutsch: Call-to-Action), z. B. „Hier klicken“ oder „Link aufrufen“. Manchmal werden die Empfänger:innen sogar aufgefordert, Geld zu überweisen.

Wenn Sie eine verdächtige E-Mail als Spam markieren, wird diese in den Spam-Ordner verschoben – genauso wie alle anderen E-Mails von derselben E-Mail-Adresse. Die E-Mail verschwindet dadurch aus Ihrem Blickfeld, das Problem jedoch bleibt bestehen.

Tipps für sicheres Verhalten

Wir empfehlen, verdächtige E-Mails Ihrer Organisation zu melden. Dann kann sich das IT-Team mit dem Problem befassen und die Bedrohung abwenden.

Mit folgenden Tipps sind Sie auf der sicheren Seite:

- Befolgen Sie den Prozess Ihrer Organisation zur Meldung verdächtiger E-Mails. Schützen Sie Daten, indem Sie sich an Cybersicherheitsprotokolle halten.
- Wenn Sie sich nicht sicher sind, wie Sie Ihrem IT-Team die E-Mail melden sollen, belassen Sie sie in Ihrem Posteingang und bitten Sie eine:n Vorgesetzte:n um Unterstützung.
- Wenn Sie sich nicht sicher sind, ob es sich bei der E-Mail um Spam oder einen Phishing-Angriff handelt, melden Sie Ihrem IT-Team die E-Mail (es veranlasst alle weiteren Schritte).

