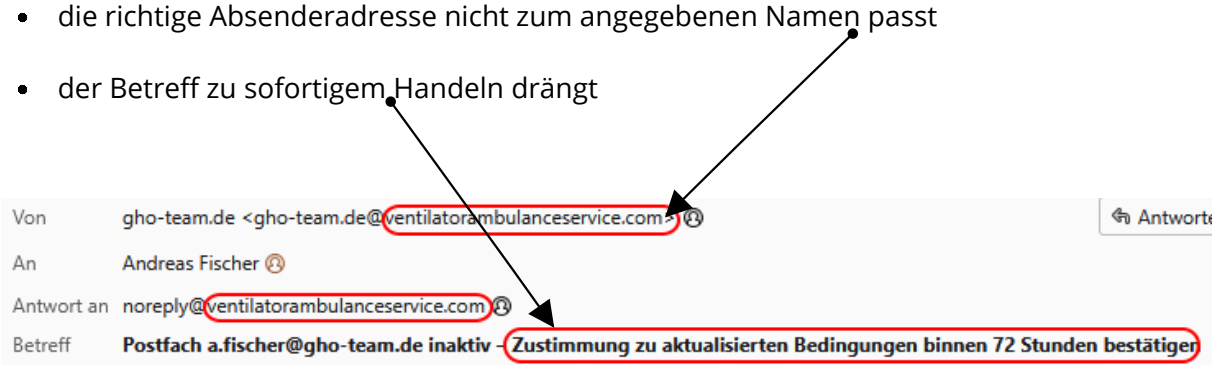
Nicht jede E-Mail kommt wirklich vom angegebenen Absender und so manche elektronische Nachricht verfolgt unlautere Ziele.

Schädliche E-Mails erkennen

Man erkennt derartige E-Mails meist daran, dass:

- die richtige Absenderadresse nicht zum angegebenen Namen passt
- der Betreff zu sofortigem Handeln drängt



Mögliche Schäden

Derartige E-Mails werden meist mit dem Ziel verschickt, die persönlichen Login-Daten oder das Adressbuch usw. zu kopieren. Gelegentlich wird darüber auch Schadsoftware auf dem PC, Tablet oder Smartphone übertragen.

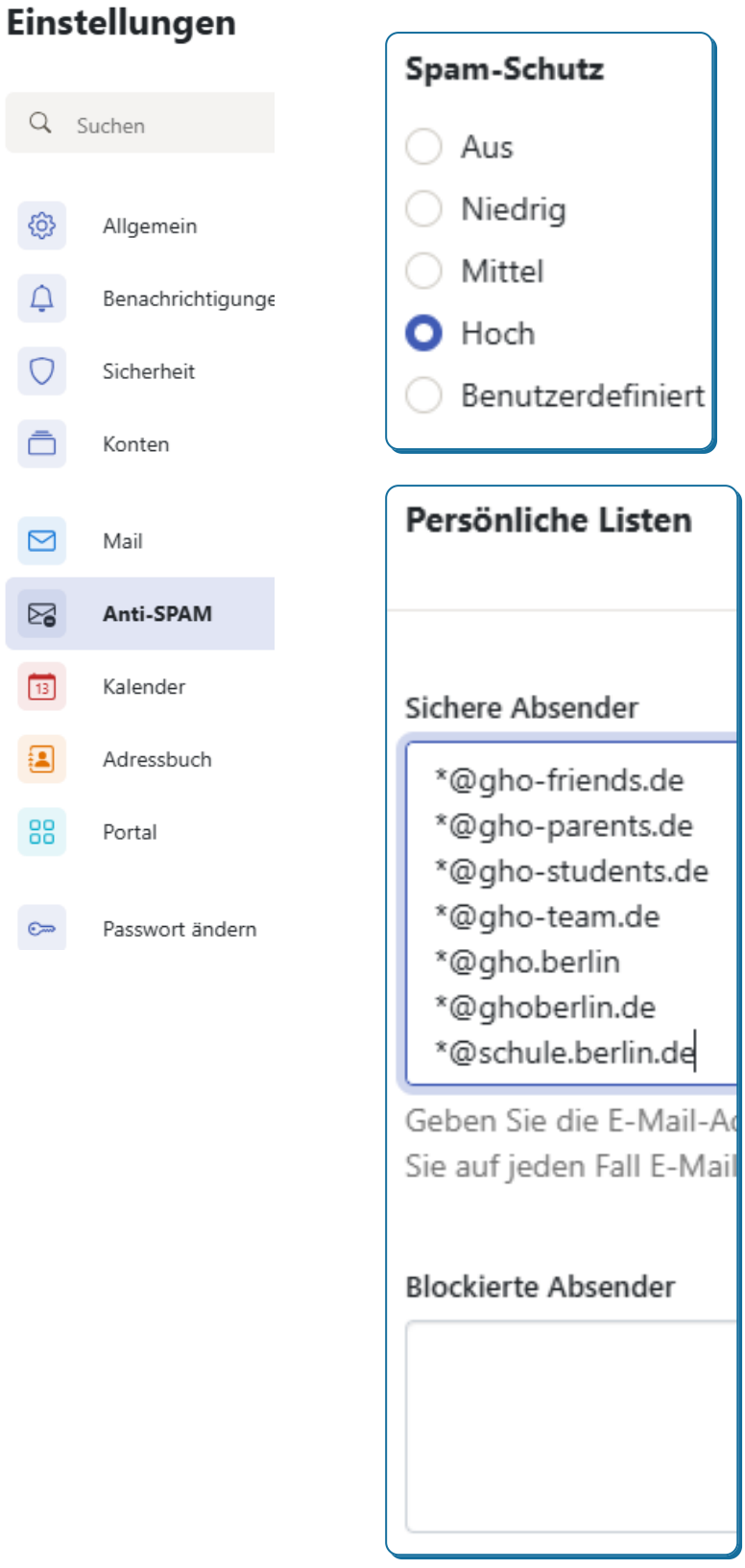
Angreifende sind manchmal sogar in der Lage, das Postfach zu kapern und im Namen der eigentlichen BesitzerIn E-Mails zu verschicken, meist Massen-E-Mails.

Massen-E-Mails führen dazu, dass die eigene Domain, z.B. gho-team.de, auf schwarzen Listen auftaucht und eigene Nachrichten (auch die von KollegInnen) nicht mehr zuverlässig zugestellt werden.

Richtiger Umgang mit schädlichen E-Mails

- Prüfe bei jeder E-Mail, ob sie wirklich vom Absender ist.
- Kannst Du dem Absender vertrauen?
- Sei äußerst kritisch, falls der Betreff zu sofortigem Handeln aufruft.
- Lösche derartige Nachrichten am besten direkt.
- Hast Du die Nachricht bereits geöffnet, klicke keinesfalls auf eingebettete Links.
- Hast Du doch auf einen Link geklickt, fülle kein Formular aus.
- Bist Du Dir unsicher, ob schon etwas schlimmes passiert sein könnte, dann ändere umgehend Dein E-Mail-Passwort.

SPAM bei IONOS (gho-team.de, gho-friends.de usw.) konfigurieren



Zusammenfassung (mit Hilfe einer KI erstellt)

Um mit Spam- und Phishing-E-Mails umzugehen, sollten Sie verdächtige E-Mails nicht öffnen, Anhänge niemals herunterladen und keine Links klicken. Reagieren Sie nicht auf die E-Mails, sondern löschen Sie diese. Wenn Sie unsicher sind, überprüfen Sie die Behauptungen telefonisch oder direkt auf der offiziellen Website, anstatt auf die E-Mail zu reagieren.

Sofortmaßnahmen bei verdächtigen E-Mails
Nicht öffnen: Öffnen Sie keine E-Mails, bei denen Sie den Absender oder den Inhalt anzweifeln.
Nicht klicken: Klicken Sie nicht auf Links in verdächtigen E-Mails. Bewegen Sie stattdessen den Mauszeiger über den Link, um die tatsächliche Zieladresse zu sehen, bevor Sie klicken.
Keine Anhänge öffnen: Anhänge können Schadsoftware enthalten. Öffnen Sie keine Dateien, auch keine vermeintlich harmlosen wie Word-Dokumente oder Excel-Listen.
Nicht antworten: Antworten Sie niemals auf Spam-Mails. Die Betrüger sehen so, dass Ihre E-Mail-Adresse aktiv ist, was zu mehr Spam führen kann.

Verifizierung und Meldung
Überprüfen Sie über andere Kanäle: Wenn eine E-Mail angeblich von einer Bank oder Behörde stammt, rufen Sie diese Institution direkt an, anstatt auf Links zu klicken oder persönliche Daten preiszugeben.
Meldung bei den Verbraucherzentralen: Leiten Sie Phishing-Mails an phishing@verbraucherzentrale.nrw weiter, um bei der Erkennung zu helfen.
Meldung an die offizielle Institution: Schicken Sie die E-Mail idealerweise auch an den tatsächlichen Anbieter, um ihn zu informieren.

Präventive Maßnahmen
Spam-Schutz aktivieren: Nutzen Sie den integrierten Spam-Schutz Ihres E-Mail-Providers und aktivieren Sie ihn gegebenenfalls.
Regelmäßige Updates: Halten Sie Ihr Betriebssystem und Ihre Programme immer auf dem neuesten Stand.
Persönliche Daten schützen: Geben Sie persönliche Informationen wie Passwörter oder Kreditkartennummern niemals per E-Mail preis.