TRUSTED DIALOG IT-SICHERHEITSEMPFEHLUNGEN

für ein jederzeit sicheres E-Mail-Marketing

Stand: Januar 2025

WARUM IST IT-SECURITY SO WICHTIG?

In Zeiten wachsender Cyberbedrohungen wie Phishing, Malware und Datenmissbrauch ist es entscheidend, Ihre IT-Systeme und sensiblen Daten umfassend zu schützen.

Mit den folgenden, gezielten Sicherheitsempfehlungen können Sie Ihre E-Mail-Kommunikation absichern und die Zuverlässigkeit Ihrer digitalen Prozesse gewährleisten.

ALLGEMEINE IT-SICHERHEITSEMPFEHLUNGEN (1/2)

- **Zwei-Faktor-Authentifizierung einsetzen**

  Bitte achten Sie darauf, dass bei allen Userkonten, die Zugriffsrechte auf kritische Systeme wie z.B. das E-Mail-Versandsystem haben, bei Möglichkeit eine Zwei-Faktor-Authentifizierung aktiviert ist.

- **Sichere Passwörter wählen**

  Achten Sie auf die Verwendung sicherer Passwörter mit mind. 12 Zeichen, bestehend aus einer Mischung von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Vermeiden Sie triviale Passwörter (z.B. „NameDerTochter1995“), verwenden Sie stattdessen Passwort-Manager zur Erstellung zufälliger Passwörter. Verwenden Sie genutzte Passwörter nicht wieder, auch nicht für andere Zugangskonten.

- **Passwörter regelmäßig aktualisieren**

  Passwörter mit weniger als 15 Zeichen sollten spätestens alle 6 Monate geändert werden, Passwörter mit 15 oder mehr Zeichen sollten spätestens alle 24 Monate geändert werden. Benutzerkonten, die ausschließlich mit Mehrfaktorauthentifizierung genutzt werden können und deren Passwörter 12 oder mehr Zeichen haben, müssen nicht periodisch geändert werden.

- **Zugangsdaten sicher speichern**

  Speichern Sie Zugangsdaten stets verschlüsselt (d.h. nicht im Klartext) an einem sicheren Ort, z.B. mit einem geschützten Passwort-Manager (Beispiele: Keepass oder Passbolt). Falls kein Passwortmanager zum Erstellen genutzt wird, sollte beim "selbst ausdenken" auf sogenannte „Passphrases“ gesetzt werden. Notieren Sie Zugangsdaten nicht auf Papier.

- **Unbeobachtete Eingabe von Login-Daten**

  Achten Sie vor der Eingabe von Login-Daten immer darauf, dass Sie nicht beobachtet werden, dies gilt insbesondere in der Öffentlichkeit. Verwenden Sie unterwegs eine Sichtschutzfolie für Ihren Bildschirm, um den Einblick auf Ihre Bildschirminhalte durch Dritte zu erschweren.

- **Nach der Nutzung ausloggen**

  Loggen Sie sich aus, sobald Sie das jeweilige System nicht mehr verwenden um einen Missbrauch durch das sogenannte „Session-Hijacking“ zu erschweren. Wo möglich sollten Sie ein automatisches Ausloggen nach Ablauf einer bestimmten Inaktivitätszeit einstellen.

ALLGEMEINE IT-SICHERHEITSEMPFEHLUNGEN (2/2)

- **Ungenutzte Konten deaktivieren**

  Achten Sie darauf, dass ungenutzte Konten (z.B. Konten ehemaliger Mitarbeitenden), ab dem Tag, an dem diese nicht mehr benötigt werden, deaktiviert bzw. gelöscht werden und keine Zugriffsrechte insbesondere zu kritischen Systemen mehr haben.

- **Userkonten nicht teilen**

  Zugänge sollten nicht zwischen Mitarbeitenden geteilt werden. Legen Sie für jede Person einen eigenen Zugang mit eigenem Passwort an.

- **Systeme aktuell halten**

  Nutzen Sie für kritische Systeme und Computer/Laptops der Mitarbeitenden nur Hard- und Software, die regelmäßige (Sicherheits-)Updates erhalten. Installieren Sie verfügbare Sicherheitsupdates schnellstmöglich, notwendige Neustarts sollten umgehend oder zumindest noch am gleichen Tag der Installation erfolgen.

- **Auf eine verantwortungsvolle Rechteverteilung achten**

  Gemäß dem Least-Privilege-Prinzip sollten Mitarbeitende nur die Zugriffsberechtigungen haben, welche zum Ausüben ihrer Tätigkeit benötigt werden.

- **Anti-Viren-Software aktualisieren**

  Führen Sie regelmäßige Virenscans durch und achten Sie auf eine stets aktuelle Virensignatur. Eine veraltete Anti-Viren-Software bietet möglicherweise keinen verlässlichen Schutz vor Viren, Trojanern und anderer Schadsoftware.

- **Computer sperren**

  Achten Sie darauf, dass Zugangsgeräte wie Laptops und PCs niemals durch Unbefugte genutzt werden können. Zugangsgeräte sollten Sie vor dem Verlassen unmittelbar sperren oder vollständig ausschalten.

- **Sichere Netzwerke nutzen**

  Achten Sie darauf, sich ausschließlich mit sicheren (WLAN-)Netzwerken zu verbinden. WLAN-Netzwerke sollten mindestens mit WPA2, besser WPA3 verschlüsselt sein.

- **Auf Phishing-Versuche achten**

  Hinterfragen Sie Handlungsaufforderungen in erhaltenen E-Mails, insbesondere wenn diese Sie um Eingabe Ihrer Zugangsdaten bitten. Prüfen Sie E-Mails zunächst auf Legitimität, bevor Sie auf Links klicken oder E-Mail-Anhänge öffnen. Seien Sie ebenso misstrauisch, wenn Sie telefonisch um Mitteilung personenbezogener Daten oder Zugangsdaten gebeten werden.

E-MAIL-MARKETING IT-SICHERHEITSEMPFEHLUNGEN

- **Einsatz einer dedizierten Subdomain**

  Verwenden Sie für den Versand Ihrer E-Mail-Kommunikation (Newsletter und Transaktionsmails wie z.B. DOI- oder Bestätigungsmails) eine dedizierte Subdomain. So schützen Sie die Reputation Ihrer Hauptdomain am besten.

- **Versand von 1:1-Kommunikation mit trustedDialog**

  Falls über die für trustedDialog aufzuschaltende DKIM-Domain in Ihrem Unternehmen auch Mitarbeitende 1:1-Kommunikation über E-Mail-Programme wie z.B. Outlook versenden, dann schalten wir einzelne Absenderadressen gerne für trustedDialog frei.
  Voraussetzung ist, dass in der DKIM-Signatur ein sog. i-Tag hinterlegt ist. Diesen legen wir in unserem System an und ermöglichen Ihren Mitarbeitenden somit auch 1:1-Kommunikation mit trustedDialog zu versenden. Sollten Sie keine Möglichkeit haben, einen i-Tag einzubinden, geben Sie bitte kurz Bescheid.

  Auf diese Weise reduzieren wir gemeinsam das Risiko, dass etwaige kompromittierte oder gar mutwillig missbrauchte Mitarbeitendenaccounts genutzt werden können, um Spam- oder Phishing-E-Mails mit trustedDialog zu signieren.

KONTAKT

Sie haben noch Fragen?

Kontaktieren Sie uns jederzeit
via **E-Mail** unter:

trusteddialog-pm@uim.de