united internet media

TRUSTED DIALOG
IT-SECURITY RECOMMENDATIONS

General IT-security information for secure email marketing at all times

IT-SECURITY RECOMMENDATIONS (1/4)

- **Use two-factor-authentification**

  Please ensure that two-factor-authentication is activated for all user accounts that have access rights to critical systems such as the email dispatch system, if possible.

- **Choose secure passwords**

  Make sure you use secure passwords with at least 12 characters, consisting of a mixture of upper- and lower-case letters, numbers and special characters. Avoid trivial passwords (e.g., “NameOfYourDaughter1995”), instead use password managers to create random passwords. Do not reuse used passwords, not even for other access accounts.

- **Update passwords regularly**

  Passwords with less than 15 characters should be changed every 6 months at the latest, passwords with 15 or more characters should be changed every 24 months at the latest. User accounts that can only be used with multi-factor-authentication and whose passwords have 12 or more characters do not need to be changed periodically.

IT-SECURITY RECOMMENDATIONS (2/4)

- **Save access data securely**

  Always store access data in encrypted form (i.e., not in plain text) in a secure location, e.g., with a protected password manager (examples: Keepass or Passbolt). If no password manager is used to create passwords, you should use so called "passphrases" when "thinking up your own" passwords. Do not write down access data on paper.

- **Unobserved input of login data**

  Before entering login data, always make sure that you are not being watched, especially in public. Use a screen protector for your screen when you are out and about to make it more difficult for third parties to view your screen content.

- **Log-out after use**

  Log out as soon as you are no longer using the respective system in order to make misuse through so called "session hijacking" more difficult. Where possible, you should set an automatic logout after a certain period of inactivity.

- **Ensure a responsible distribution of rights**

  In accordance with the principle of least privilege, employees should only have the access authorizations they need to carry out their work.

IT-SECURITY RECOMMENDATIONS (3/4)

- **Deactivate unused accounts**

  Make sure that unused accounts (e.g., accounts of former employees) are deactivated or deleted from the day they are no longer needed and no longer have access rights, especially to critical systems.

- **Do not share user accounts**

  Access should not be shared between employees. Create a separate account with a separate password for each person.

- **Keeping systems up to date**

  Only use hardware and software for critical systems and employee computers/laptops that receive regular (security) updates. Install available security updates as quickly as possible; necessary restarts should be carried out immediately or at least on the same day as installation.

- **Update anti-virus-software**

  Carry out regular virus scans and ensure that your virus signature is always up to date. Outdated anti-virus-software may not provide reliable protection against viruses, Trojans and other malware.

IT-SECURITY RECOMMENDATIONS (4/4)

- **Lock the computer**

  Make sure that access devices such as laptops and PCs can never be used by unauthorized persons. Access devices should be locked immediately or switched off completely before leaving.

- **Using secure networks**

  Make sure you only connect to secure (WLAN) networks. WLAN networks should be encrypted with at least WPA2, preferably WPA3.

- **Watch out for phishing attempts**

  Question requests for action in emails you receive, especially if they ask you to enter your access data. Check emails for legitimacy before clicking on links or opening email attachments. Be equally suspicious if you are asked to provide personal data or access data by telephone.

CONTACT

Do you have any questions?

Contact us at any time by **email** at:

trusteddialog-pm@uim.de