tdmgroup™
we make IT possible

Email Security Awareness & Best Practices

Email Security has always been a priority for all businesses; it is a collective measure to secure the access and content of email accounts. As important as enterprises and companies having protective software against such attacks; it's critical for end users themselves to follow various techniques and steps in order to achieve best possible security to their sensitive information.

> **"If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees."**

Passwords

Use secure and unique passwords. Essentials for a strong password are:

- Use upper and lower case letters.
- Use two or more numbers and special characters.
- Do not use dictionary words.
- Preferably longer than 10 characters.
- Use random numbers and letters rather than words.
- Never use your birthday, hometown, school, university, or company name.
- Avoid common letter-number substitutions (Pa$$wOrd).

Do not share password:

- Avoid writing down your password and leaving it on your desk or a public location.
- Avoid typing down your password on notes on your desktop.
- Avoid sharing your password with your colleagues.

Clear Your Cache and turn off the "Save Password" Feature in your browsers.

- By keeping the feature disabled; All accounts will require your credentials every time you try to log-in. Thus, even if your laptop was borrowed by one of your colleagues, friends, random strangers at a coffee house or reported as lost; your data will be safe.

Privacy

Don't include sensitive information in your email messages.

- If you must, you can break sensitive information into two or more parts, then send each part in a separate email or different communication method. That at least makes it harder for hackers to get the information they need to do damage.

Don't use your business email to sign-up to any social media platforms.

Avoid accessing emails from public Wi-Fi as much as possible.

Public Wi-Fi locations (coffee shops, libraries, airports, hotels, etc.) are convenient but they're not secure at all. Most networks are not encrypted and often filled with cyber-predators ready to hijack your session and spy on you.

If you had no other choice; please follow the below steps while you're connected:

- Don't stay permanently signed in to accounts. When you've finished using an account, log out.
- Try not to use any of your sensitive information, such as banking details, social security number, etc.
- If you can, log in using a Virtual Private Network (VPN).
- Always Use "HTTPS" option on all your frequently used websites.
- Do not accept any download or access request you are not sure of it's source in general, and specially not while you are connected to a public Wi-Fi connection.
- Personally identifiable information such as data that falls under GDPR compliance should not be sent by email without encryption.

Phishing

Be extremely careful about opening attachments and hyperlinks:

- Opening email attachments from unknown sources could result in infecting your computer with harmful viruses.

  The attachment could also be loaded with scripts and codes that allows the sender to hack into your computer.

  Just remember; if you don't know the sender, don't open the attachment.

- Always verify the legitimacy of the senders before opening any attachments or clicking on links.

Don't reply to spam or phishing schemes.

- Responding to spam emails will only rise the potential of jeopardizing your information as well as the company's.

  Thus, we should not reply to any suspicious email addresses.

Exercise caution when enabling macros.

- A macro is a series of instructions used in Microsoft Office apps to accomplish tasks automatically. Hackers see that as a vulnerability, so they send you macro-infested document where it's designed to download malware or preform other corrupted tasks desired by the hacker.

  Hence, even if you receive a document from a trusted source; make sure to contact the sender to ensure if there is any need for enabling macros and whether it was tested or not.

General Tips

Turn on Two-Step Authentication Policy

- Two-factor authentication (or Multi factor authentication) is an additional safety layer for your corporate related accounts, used to enhance the security level on your data. Once the application accepts the username and password; it will send a verification code to another device, such as your mobile number or an additional email address.

If you lose a USB drive that happens to contain confidential data and corporate sensitive information, please make sure to notify your team-lead as well as your IT department.

Set up recovery information.

- In case you forgot your credentials (username/password) or it was locked due to multiple failed-login-attempts; you can set up security questions beforehand to avoid being locked out completely and losing your email.

Contact us for improved email continuity & security

0808 129 22 99 | hello@tdmgroup.net | www.tdmgroup.net