

5 Best Email Security and Safety Tips That You Should Know About

TechRounder PDF Edition

Live article:

<https://www.techrounder.com/security/5-best-email-security-and-safety-tips-that-you-should-know-about/>

By Vipin PG | Published March 13, 2024 | Updated March 9, 2026 | Format: Analysis | 3 min read

In brief

Protect your email security by avoiding messages from unknown senders, never clicking suspicious links or attachments, and refraining from sharing personal information like credit card numbers or addresses through email.

Taking care of your online security is an important part of being a modern person, as internet threats are increasing daily. Almost every person who uses the internet is exposed to some security threat, and even though most of us are well aware of the importance of staying safe online, many of us do not take the necessary precautions regarding email safety. To help you, we have compiled a list of the best email security and safety tips you should know about.

Don't Open Emails from People You Don't Know

Since everybody has an email account, knowing the dangers of email scams is important. Every day, thousands of people worldwide fall victim to various email scams, in which scammers attempt to trick users into revealing their personal information or infecting their computers with viruses. A standard method employed by scammers nowadays is by sending emails pretending to be from a legitimate source or company. However, most of these emails are spoofed and scam emails that are not from a legitimate source.

If you ever receive an email from someone you don't know, it is best to be cautious when opening the email or the links it contains. If you are in doubt, it is best to contact the said person or organization to confirm the received email or visit the organization's official website, or even a similar reliable source like Capcut official website, to confirm the email address.

Never Click Unknown Links or Email Attachments

Cyber attackers and scammers are becoming more and more proficient in scamming people. The increasing sophistication of email scams has made it hard for an average person to know what's safe to click and what's not. However, one rule that can keep you safe is to avoid clicking on links or attachments in emails from people you don't know.

Scammers may send you links and attachments pretending to be your friends or family members. If you ever receive a suspicious email with a link or attachment, it is best to delete the email without opening any links or attachments that it contains.

Avoid Sharing Personal Information

In the digital world, one has to be very careful with their personal information and always exercise caution. Scammers are always on the lookout for individuals' personal and private information. You should ensure you don't share important information like your address, phone number, credit card, or social security number with anyone through email, as this information can be used to steal your identity. Whenever you send an email, it is best to be safe and avoid sending sensitive information through emails.

Have Reliable and Updated Antivirus Software

Antivirus software has become increasingly important to ensure your smartphone or computer is safe and secure from online threats. Antivirus software can protect against the online dangers of malicious software and apps by providing real-time protection, which can block any malicious attacks before they happen. Therefore, it is essential to download a reliable antivirus program from Google Play, App Store, or the Internet to keep your device safe.

Use Different Emails for Different Purposes

A common mistake many people make regarding email security is using the same email for different purposes. Using the same email for different purposes, such as professional and personal, can put you at risk. You should use different emails for different purposes because professional emails are the ones that are generally accessible to the public. In contrast, personal emails are meant to be shared with close people only. That way, the emails you receive won't be linked, and you will get different emails at each address. You can decide accordingly what action you want to take.