11 Smart Ways to protect your Email Privacy

Why you should worry about email privacy?

When someone gains access to your email username and password, that person can easily collect enough personal information about you—usually via people-search sites—to steal your identity and damage your online reputation. Because it is a good money-maker, email hacking has grown into a huge industry. There's even a website where you can check to see if your account information has been compromised.

One reason cybercriminals are going after email accounts is due to the way email works. Even without being hacked, email is one of the least secure forms of communication. In fact, some have compared it to a postcard because its contents are viewable by anyone who happens upon the message during its travels. This is because email is not a direct form of communication.

Email messages pass through numerous servers, including those of the various Internet Service Providers (ISPs) and mail clients involved. And each server stores multiple copies of every message, with additional copies stored on the sender and recipient’s devices. As such, even when you delete your original email, you aren’t removing all the other copies that exist.

Even more worrisome is the fact that your email is connected to everything you do online. Nearly every time you sign up for an online service, you have to enter your email address. Once you are registered, the service usually sends you an email containing your password information and terms of service.

Therefor, hackers who have access to your email inbox automatically gain entry to your accounts on all of these websites. This can be especially harmful if hackers obtain the login credentials to your financial accounts or your business’s website, where you store confidential data about your customers and employees.

And don’t forget that once someone has your email username and password, they can see everything you’ve ever sent via email. This includes pictures, tax forms, contracts, and personal communication—all of which can be used against you.

Email privacy tips

You should always be concerned about your privacy when using email, but you don’t have to abandon it entirely to keep your information secure. Instead, you can follow these tips to mitigate the risks:

1. **Use a strong password:** Your email password is the only thing standing between your private personal information and Identity theft. Therefore, it needs to be as strong as possible. The key ingredients of a strong password are length (with longer being better); a mix of letters (upper- and lowercase), numbers, and symbols; no connection to your personal data; and no dictionary words.
2. **Beware of public Wi-Fi:** Hackers often set up fake hotspots that enable them to intercept and store people’s personal data. This gives them access to a host of information, including email usernames, passwords, credit card numbers, bank account details, and more. Although many people know the dangers of using public Wi-Fi, research from BullGuard found that two-thirds of individuals have configured their devices to connect to the nearest hotspot automatically. To stay safe, don’t use public Wi-Fi, especially if you are signing in to online banking, checking your email, or doing anything else that might reveal sensitive information.
3. **Protect your address:** While your email address is hardly a secret (as everyone can see it on each email you send) there’s no reason to give it out when you don’t need to. For example, don’t post your email address on social media or include it in blog post comments because cybercriminals are constantly scraping these sources for new victims.
4. **Lock your screen:** Don’t leave your email account visible for others to see. Even if you’re just stepping away for a minute, you should always lock your desktop. Otherwise, a passerby could read your mail or (if they are particularly evil) reset your password. On a Windows machine, hold the Windows key and press “L” to lock the desktop. On a Mac, you can use Command+Control+Q or Control+Shift+Powerbutton. If your Mac has an optical drive, click Control+Shift+Eject.

5. **Sign out every time:** In addition to locking your screen, it's always a good idea to sign out of your email account whenever you are not using it. This is especially important if you are using someone else's computer or if another person has access to yours.
6. **Don't fall for phishing scams:** An email or text message that tricks you into revealing your private information is called a phishing scam. Thousands of these types of cyber attacks occur every day, and many are successful. In fact, the FBI reports that, in 2017 alone, phishing schemes cost Americans $30 million. Google has even gone on record saying that phishing attacks are the "greatest threat" to its users. To avoid becoming a victim, never click on any email links. If you receive a message from a company you do business with, contact the firm to verify that it sent the email before responding.
7. **Encrypt your connections:** To safeguard your personal information from identity thieves, you need to encrypt the connection between your computer and your email server. This prevents personal data like usernames and email addresses from being intercepted by eavesdroppers. (An encrypted site's address will start with https:// instead of http://.) Some mail services, like Gmail and Outlook, encrypt your connection automatically, while others require you to alter your security settings manually. A good way to ensure your messages are always encrypted is to use a VPN.
8. **Use a secure email service:** Once your messages reach the mail server, they're readable by anyone in the relay chain between you and your recipient. To solve this problem, you'll need to encrypt the actual content of your emails with a secure email service like Hushmail, CounterMail, or ProtonMail.
9. **Use two-factor authentication:** With this extra security measure, anyone trying to log into your account has to prove they're you by entering a temporary passcode that your email provider sends to your phone. Another advantage to this feature is that you'll know that someone else is trying to log into your account when you receive passcode messages when you aren't trying to log in.
10. **Understand your service provider's TOS:** In order to plug all the security holes in your email account, you need to first know what they are. And the way to find out is to read your email provider's Terms of Service. Does it encrypt messages on its server? Does it have any defenses against brute-force attacks? Does it promise to protect your data? While you might assume that your email provider values your privacy, there's a good chance it doesn't see privacy in the same way you do. Google, for example, lets third-party developers read your emails.
11. **Don't send personally identifying information via email:** The easiest and most effective way to keep your vital data protected is to not share it electronically in the first place. Instead, communicate your private information in person with the individual or organization who requires it.

Reference: https://www.reputationdefender.com/blog/privacy/11-smart-ways-to-protect-your-email-privacy