Survivors' Guide to Email

Email can be a convenient way to send a message that can include pictures, documents, or other files as attachments. You can send emails through a web browser, an app, or email software. Many people use free email accounts connected to cloud accounts such as Gmail, Apple, or Microsoft (also known as Outlook or Hotmail), or through an employer or school. Your employer or school may use a provider such as Gmail or Microsoft for staff and student email addresses, even if the email addresses use the organization's own name rather than something like "gmail.com" or "outlook.com."

How Email Could Be Used Against You

An abusive person may be able to read your email if they can access your account, have installed spyware on your phone or computer, or have set up your account to secretly forward emails to their own account.

An abusive person can send harassing messages by email, either in the message itself or in any attachments, or they could create a fake email account to trick you into opening messages or to hide their identity. They could also insert a *tracking pixel* into emails they send you, which could give them information about whether you read the email and your location when you read the email. Tracking pixels can be inserted into emails using sales & marketing tools, or by adding code into an email manually – they do not require someone to have physical access to your device. The "Strategies to Counter Email Harassment" section of this resource talks about ways to address these forms of harassment.

Prioritize Safety

Use a safer device. If you think that someone is monitoring your email, use a different device or account that the person cannot access (and that they have not had access to in the past) such as a computer at a library or a friend's phone.

Get more information. Navigating violence, abuse, and stalking can be difficult and dangerous. Advocates can help you figure out options and local resources and help you create a plan for your safety. You can contact a national helpline to be connected with local resources.

General Email Privacy & Safety Strategies

- When communicating sensitive or personal information, avoid using email, particularly if the abusive person may have access to the email account or to devices used to read the emails.
- Try not to open attachments or click any links when sent from the abusive person or someone you don't know. They may contain stalkerware or other harmful software. Use an anti-virus app or software on your computer, tablet, and phone.
- Disable automatic image downloads in your emails (because images are a popular way to send tracking pixels by email). This article describes how to do that for Gmail, Outlook, and Apple Mail.
- What you do in an email message can possibly be tracked. You can use an email tracker blocking tool like Trocker, which blocks a person's ability to use tracking pixels to see how you engage with the emails they send. This prevents them from using tracking pixels to learn your IP address (general geographic location), the time you read an email, or what technology you used to read the email.

- If you need to share documents or pictures, use an online picture or document sharing site.
- You can get a new email account the abusive person doesn't know about. In addition to the free options mentioned at the beginning of this resource, you might consider using a more secure email service like Proton Mail for your most sensitive emails.
    - You can have more than one email, and use each account for different purposes. For example, you could use one account for banking or work, and another for online dating.
    - Do not access the new email account on a computer or device that is being monitored.
    - Use strong passwords for new accounts, and store them safely in a password manager. Read to learn more about how to do this.
    - Consider keeping the old account to keep the evidence.
        - If you do this, you may want to log into the old account from a safer device, , so that the other person cannot get into the account and delete the evidence.

Strategies to Counter Email Harassment

- If you receive threats or harassment by email, you can document the messages.
    - While it may be tempting to delete the message, some of the best evidence is in the original email itself. Keeping the original emails and documenting what is happening can help if the harassment continues and you decide to pursue legal options in the future.
    - If the other person has access to your account, you may want to forward a copy to another email account that the abusive person

does not have access to, in case the original gets deleted. This other email account should only be used to save the forwarded emails, to minimize the chance of it being discovered.

  - You can also print copies of emails, but be sure to include the full email header, which you can find using these instructions.

- You can block a specific email address, or set up a filter so the messages go to a separate folder or another account.

Supported by US DOJ-OVW Grant No. 15JOVW-21-GK-02216-MUMU. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.