NNEDV

# Safety & Privacy Tips for Older Technology

Talk of technology abuse and technology privacy often focuses on the newest devices, services, and platforms. Yet, older technologies, such as cordless phones, and fax machines, are not only still in use, but they are still very relevant for survivors of abuse. Some abusive people use older technology to stalk and harass, and older technology can present privacy risks that can impact safety. Because of this, it is important to understand how older technology can be misused and how to minimize risks.

## Prioritize Your Safety

This resource will look at some safety considerations for a few older technologies. Before diving into that list, a few notes on safety:

- **Get help.** Navigating violence, abuse, and stalking can be difficult and dangerous and you don’t need to do it alone. Advocates can help figure out options and local resources can help you create a plan for your safety. You can contact a national helpline to be connected with local resources.

- **Trust your instincts.** Abusive people are often determined to maintain control, and technology is one way they do this. There are steps you can take to secure your devices, apps, and accounts. There isn’t one “right” way to respond. What works for someone else may not work or be safe for you.

- **CAUTION**: Making changes will often alert the other person. They might force you to unlock your phone or share your passwords. They might become more abusive. Making changes could also erase evidence.

## Cordless Phones

While the use of cordless phones is on the decline, they are still around and sometimes because they can increase safety. It's important to note their differences and where there can be a privacy risk versus a safety strategy. In areas where cell phone signal is unreliable, it can be helpful to have a landline phone in the event of an emergency. However, some older cordless phones can be easily intercepted, meaning someone else can listen in on the conversation. Cordless phones transmit conversations wirelessly between the base unit and the hand-held phone. Older cordless phones may be analog, meaning that the sound waves of your voice are sent, whereas newer digital phones send information that may be encrypted or scrambled. Calls on the older analog phones could be intercepted by scanners, baby monitors, or other cordless phones. Newer home phones, cordless or otherwise, may transmit calls through the internet (called VoIP), and use encryption to secure conversations.

*Safety Strategies*

- Switch to a corded phone or a safe mobile phone (one you don't believe could be monitored remotely), before exchanging sensitive information.
- If moving to a corded phone, unplug the cordless base unit after the call has been transferred to ensure that the conversation won't continue to be broadcasted and overheard.

## Faxes

Fax machines are still used in businesses, legal services, and courts to send documents, either using a phone line or the internet. The information at the top of the fax is called a header, and it includes the sender's fax number. This could be used to determine location if someone does a reverse phone number look-up. Most fax machines have hard drives that keep a log of the faxes that have been sent and received, and often also a copy of the fax itself. Someone else might be able to see your fax at a later time. Electronic faxes (e-faxes) are sent through the internet as email attachments and, like regular email, could be intercepted if someone has access to the email account.

*Safety Strategies*

- Sometimes a fax may be forwarded beyond the person you're sending it to. For example, a fax sent to your attorney could later be sent on to the abusive person's attorney.
    - You can request that the header information be removed before forwarding to protect your privacy.
    - Before using a public fax machine (such as at a store), consider the information being faxed and determine if using it will impact your privacy risks. If it's not something you feel comfortable sending from that location, talk to a victim service provider about other options.
- Avoid sending personally identifying or sensitive information in an e-fax.
- If a regular fax to a machine in a place with multiple people, call ahead so the person you're sending it to know to expect it and can remove it immediately.

### TTY & Relay Services

TTY stands for teletypewriter. A TTY is a machine for people who are Deaf or hard-of-hearing that connects to a phone line. TTY can also be used through an app or computer. Relay is a free service where an operator facilitates a conversation between a person who is using a TTY and someone else without a TTY. The call log or transcripts of TTY might be saved on paper or electronically. Abusive people who monitor TTY calls or a relay conversation might see or record this information. Since TTY communication is written, it can also be easier for an abusive person to pretend to be someone else.

*Safety Strategies*

- For privacy, you could regularly clear TTY history or destroy the paper print out. However, an abusive person might notice, which could be a safety risk.
- Alternately, consider saving the transcript of a TTY conversation as evidence of harassment or abuse.
- To avoid impersonation, set up a code word or phrase so other people know it's you.
- If possible, use a "safer" TTY, device, or computer that the abuser doesn't have access to, or meet in person to discuss sensitive information.

**Keystroke Logging Hardware**

These are devices that can record everything typed on a keyboard. Keystroke logging hardware can look like a small connector piece or plug that connects the keyboard to the computer, something plugged into a USB port, or even an external keyboard. Keystroke data can include passwords, which could give someone access to email, bank accounts, and more.

Someone might have installed one if they accessed or fixed your computer, or gave you a new part for your computer. Information recorded by keystroke logging hardware can be read remotely or in person.

*Safety Strategies*

- Look to see if there is a device or plug attached to your computer or keyboard that you don't know about or didn't put there yourself.
- Be cautious about removing anything you find. It might alert the abusive person, or erase evidence of the abuse. You can talk with an advocate about your options and to develop a safety plan.
- If you choose to leave the keystroke logger in place, consider using a different device that the abusive person doesn't have access to such as a computer at a

library or a friend’s phone to reach out for help, access sensitive accounts, or change account passwords.

Supported by US DOJ-OVW Grant No. 15JOVW-21-GK-02255-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.