

# 8 security issues to keep in mind when recycling hardware

Here are some security concerns that you need to consider before removing your hardware and what you can really do with them.

Most of us have old electronic devices in the house. It may be that an old PC is not under warranty, an old iPad has been replaced by a new one with larger memory, or the Xbox 360 has been replaced with the Xbox One.

They still work, but you don't need them anymore. You cannot put them in the landfill because too many ingredients can be dangerous to the environment. Instead, you can consider donating them to a school, church or charity. However, it should be noted that the amount of personal data stored in these devices and whether it is safe to donate these devices.

Here are some security concerns that you need to consider before removing your hardware and what you can really do with them.

## 8 security issues to keep in mind when recycling hardware

1. Personal information
2. Financial data
3. medical record
4. Old photos
5. Social network account
6. Message
7. Contact details
8. Gaming account
9. What you can do

### Personal information

Your personal data can be stored on anything with permanent memory, including PCs, laptops, smartphones, Apple devices and game consoles.

Data may only be content such as your name, address and birth date. It seems completely harmless. But not so.

In addition to considering how much your personal information is worth on hidden and more specific deep web, dark web, think about how someone can use that data to learn more about yourself and open it. What are the

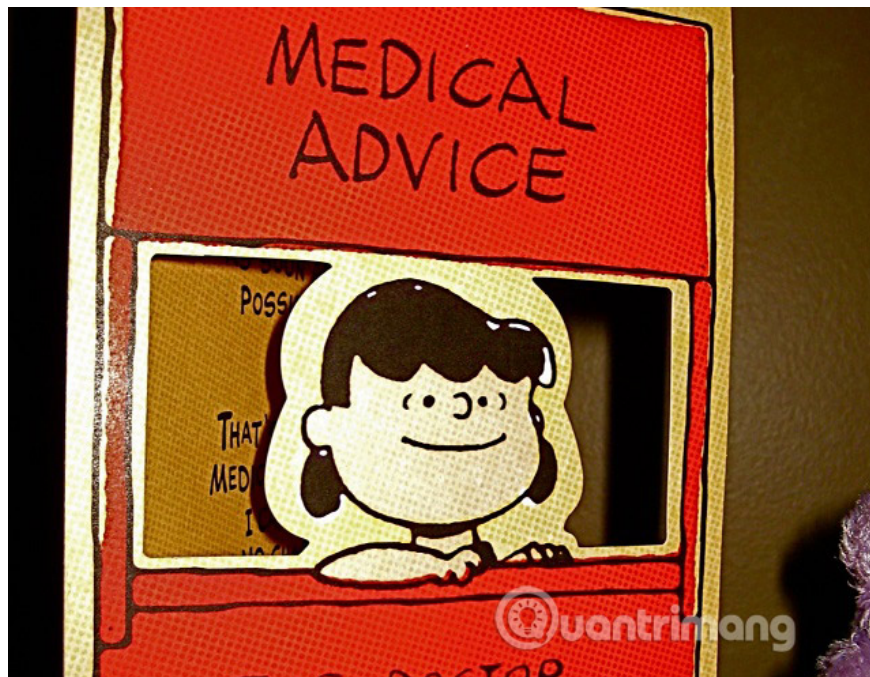
'gates'. Could that information include clues to your password? What about the answers to different security questions?

## Financial data

With Personally Identifiable Information (PII) - Personally identifiable information, the thief is likely to receive a credit card under your name. If that is not worrisome, imagine that they are also holding your financial records.

Thanks to cookies, most of your information is stored and some people can choose to save passwords in the browser on certain devices. This is bad news - especially when it comes to online banking and PayPal. Even with the smallest traces of financial data available on your device, a scammer will also be able to find and exploit it.

## medical record



The core of all worries is data reuse. Even if you throw a file in the trash, the data still exists in the hard drive (HDD), waiting for you to recover yourself (in case you realize you really need it) and someone with a bad purpose can take advantage of this.

If those files include medical information, those are certainly potential concerns.

In fact, health information theft is increasing, as such details are often collected and sold at high prices.

## Old photos

There is an increasing trend, that is, entering pictures on Snapchat or similar applications. These are things that are personal and definitely something you don't want strangers to own.

A few years ago, the problem called 'Celebgate' created a flaw. But it's not just about revealing personal things you don't want strangers to see, but it also makes you the target of sextortion.

And even if you don't have such an 'adult' document on your PC or smartphone, it's certainly scary that someone you don't know by chance of seeing your daily photos is not?

## **Social network account**



Once again, this may not seem so worrisome, but in fact, social networking accounts like Facebook, Twitter and Tumblr reveal a huge amount of details about an individual. Doing a security check will not make a difference, if your login data is still on an old drive, giving someone the chance to remotely log into Facebook and manipulate you.

Any device owned by young people is particularly troublesome. Ken Munro, from security company Pen Test Partners, warned:

'Our biggest concern is that bad guys can buy cheap tablets, already used from online auction sites and other sources. Using simple tools, they can recover children's data and passwords. This can allow bad guys to directly access the children's social network, follow up from within this account. They will have access to your child's account. "

## **Message**

Smartphones store your SMS messages on encrypted messaging applications, but that encryption only protects them between devices. Old mobile phones store that data on SIM. So simply removing the SIM card is done, why is it still not safe?



Messages are private in their nature, but they can also contain intimate photos or account details. How many of us delete messages systematically from service providers?

In some cases, **PCWorld.com** found that recycled phones still contain voicemail, messages and emails. Put all those together and you have a completely accurate picture of a person's life.

## Contact details

In case there is a problem, your address book is usually saved to both the internal memory of the mobile phone and the SIM card. Therefore it is not safe to lose your SIM card, for example, if you still keep contact details of family and friends in it.

Most people will remove the SIM card when recycling their phone, but that only prevents it from communicating online. Other information is still on the phone, and your loved ones will probably get caught up in the trouble, if they get problematic calls.

If in doubt, remove the card, then turn on the phone again and see which data you still have access to. You may be quite surprised with this information.

## Gaming account

Today, game consoles have a lot of features, so the latest Xbox and Playstation comes with a 500GB hard drive, to store all kinds of downloadable content (DLC), save game data and profile information. of some gamers. Those are private documents, especially when they're stored in SD cards and cloud services like Xbox Live.

Recycling consoles is a popular decision because it helps you get closer to owning a newer system. While some professional services will help you delete those data, you also don't want to miss something important - like an account or financial data, etc., right?

## What you can do

These potential security breaches will not prevent you from recycling your old hardware.

The first step to do is research. Find out what you can recycle, where you can remove them and consider environmental issues.

The "**Scorched Earth**" option specializes in destroying your hard drive. You often want to do this when system connections and updates are slow. This is your chance, to get rid of the old and buy a new hard drive. The same goes for some consoles like the PlayStation 3. That's one of two ways you should do it to completely destroy the information on your hard drive.

If you can't do it yourself, you can hire an expert or overwrite the data. **Permanent Eraser for Mac** (reference link: <http://www.edenwaith.com/products/permanent%20eraser/>) check the initial information 35 times and delete the file name. That is a pretty solid solution. You can also delete files from your hard drive on Windows or use Eraser, which works on Linux, safely.

#### 1. How to completely delete data on the computer?

Apple devices are often very effective when deleting all saved data. Please create a backup version on iTunes to write to a new phone, then go to **Settings> General> Reset> Erase All Content and Settings> Erase iPhone** .

It will erase your entire old device. It also destroys the digital rights management rights - DRM - in the iTunes Store, before recycling the computer. The purchase authorization also applies to some SecuROM games, which limits the number of devices you can register. And in general you are not limited by these things.

Resetting Android devices is usually not completely useful, so encryption is a safer measure of your data. In fact, it's valuable no matter which smart phone you're using.

As an additional safety measure, you can always change your password on any important account: PayPal, online banking, iTunes, email and social networks including Google Play. But don't do it on the device you're trying to remove.

Check if you are logged into Facebook on your old PC (or any other backup device), by opening **Settings> Security> Where You're Logged In** and clicking **End Activity** for any thing What else, apart from what you currently use.

How to delete information from game consoles will definitely vary, depending on the manufacturer. You should check specific websites for exact instructions for each type and note exactly what will be deleted. For example, for Wii, you need to access **System Settings** , then select **Format Wii System Memory** . Click **Format** three times. This will delete all data and downloads.

Don't forget to delete any external storage device, including USB and SD card.

Cloud services give you peace of mind, backup all your personal data safely.

But the important thing is: Turn off all cloud synchronization before deleting documents and photos. Those files will still be stored on Dropbox or any system you choose. That includes disconnecting clouds and membership with accompanying game consoles, such as Nintendo's shopping channels.

Do you have other tips to make sure all your personal information is deleted? Do you have any other concerns? And how do you recycle your old hardware? Let us know in the comments section below!

See more:

1. 5 ways to fully utilize old computers
2. 19 great ideas to take advantage of old smartphones
3. 8 ideas from the old hard drive

You finished reading the article "**8 security issues to keep in mind when recycling hardware**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

---