The Christmas gifts that keep giving (your data away)—and how to prevent this

January 5 2021, by Paul Haskell-Dowland and Steven Furnell

Credit: AI-generated image (disclaimer)

With the festive season having come to a close, consumers the world over will be playing with a variety of new tech toys.

In recent years, the most popular gadgets sold on Amazon have included a variety of smartphones, wearable tech, tablets, laptops and digital

assistants such as Amazon's Echo Dot.

And it's likely our gifting habits over Christmas reflected this. But any device connected to the internet (including almost all of the above) exposes our personal data to a host of threats.

Few of us stop to consider how our new devices may impact our digital footprint, or whether they could build new channels between ourselves and cyber criminals.

With this in mind, here are some simple tips to help you lock down your digital footprint this year.

Use more sophisticated credentials

First, when it comes to setting up a new device and/or account, you should always use a unique password—every single time.

While this task may sound painful, it's made much easier by password managers. Should your password for a particular account be stolen, at least the others will remain secure.

It's also worth checking the Have I Been Pwned? website, which can reveal whether your online credentials have already been leaked.

And even if you're using more sophisticated biometric-based approaches on a device (such as face or fingerprint login), you can still leave yourself exposed by having a weak password that can allow hackers to bypass the biometric.

Also, if you ever have to enter a credit card number or other financial details to set up an account, you may want to remove them through the service provider's site or app.

Some services require ongoing payments, but deleting stored payment details where they are no longer needed will help protect your finances. Most services will provide an option to do this, although others may require you to get in touch directly.

You don't always have to be transparent online

We constantly provide our personal information online in exchange for access to accounts and services.

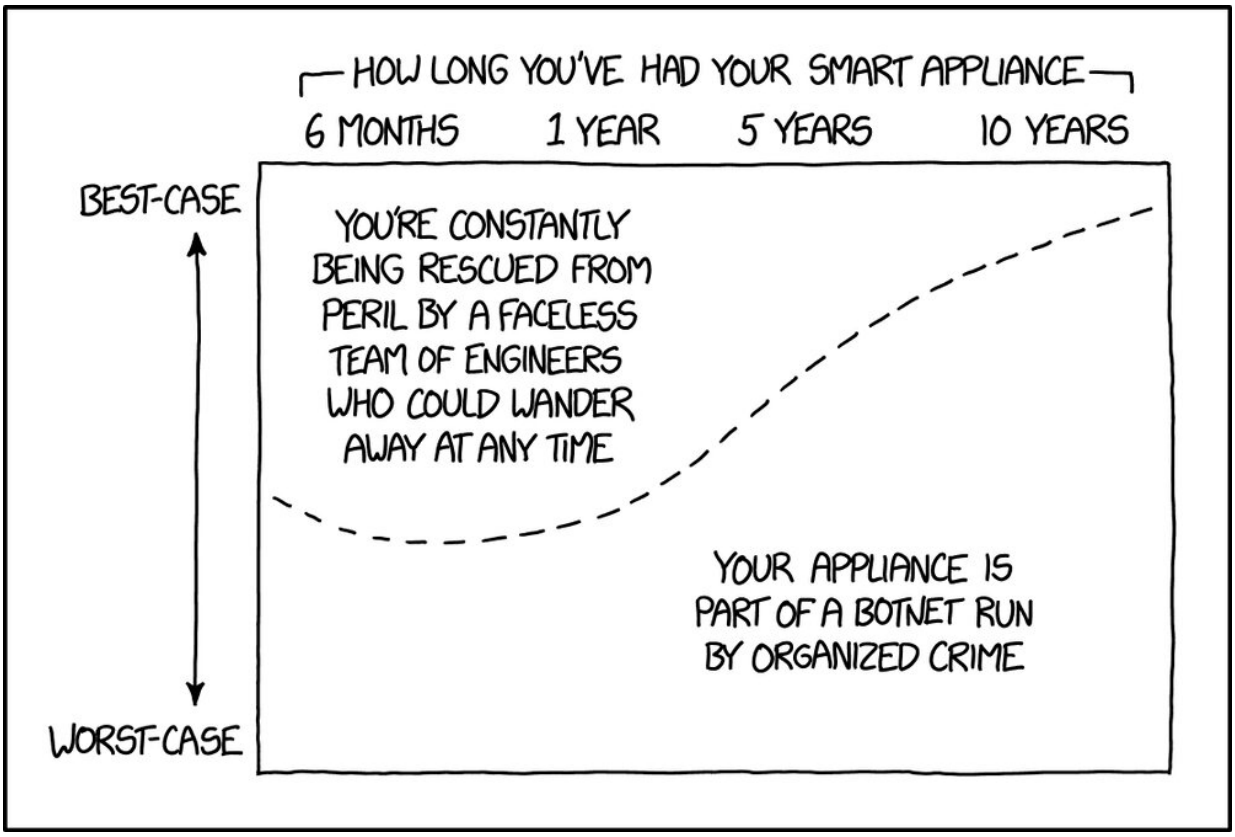
Often this includes date of birth (to validate your age), postcode (to offer regionally locked services) or details such as your mother's maiden name (to help restrict unauthorized access to your account).

Consider having a fake identity. That way, if your details are stolen, your real data will be safe.

You may want to set up a sacrificial email account, or even a temporary address (also called a "burner email") to sign onto services that are likely to spam you in the future.

Apple device users may want to explore the "Sign in with Apple" feature. This restricts the amount of personal data shared with a service is being used.

It can also hide the user's actual email address when registering—instead creating a site-specific alias that can later be blocked if necessary.



When it comes to smart home products in particular, almost all devices lose support from the vendor after a certain period (usually a couple of years). This means discontinued support and updates on security capabilities which may have once protected the device from hackers. Credit: xkcd.com/1966, CC BY

What happens to our old devices?

When new gadgets enter our lives, the old ones are often passed on to friends and family, sold to strangers, traded in, or simply recycled.

But before we discard our old devices into this growing technology mountain, we should make sure they're clear of our data. Otherwise, selling an old phone may also mean inadvertently selling your private information.

Many modern devices, particularly smartphones and tablets, have a factory reset option that removes all user data.

For devices without a distinct wipe or reset option, you can consult with the user manual or manufacturer's website (which will often have a copy of the user manual). If in doubt, there's plenty of online advice on how to reset devices.

You may need to remove or unlink the old device from your online identities, such as your Apple ID.

It may also be necessary to delete cloud-based accounts—such as Dropbox or Google Drive—set up specifically for that device. And don't forget about data stored on devices being returned to the seller (perhaps after Boxing Day sales).

A 2019 UK study examining second-hand phones on eBay found only 52% had been properly wiped or reset.

Moreover, 19% contained some form of personal information, ranging from active social media logins to bank account details.

Parental responsibility

Children (especially those in primary school) who use devices should be educated on safe internet practices and cyber safety.

While younger people are becoming increasingly tech-savvy with time, they don't necessarily know the risks associated with using internet-connected technologies.

It's important for parents to first learn about appropriate safeguards, and then remind their children of them regularly.

Don't panic

The good news is you don't need special cyber security training for each new tech purchase. The lessons above are transferable, so the key is simply to remember to use them.

There are plenty of sources for further learning, including UK Cyber Aware, the Get Safe Online initiative, and the Australian eSafety Commissioner's website.

To quote from the film The Hitchhiker's Guide to the Galaxy: "don't panic." Just think carefully about how you use (or get rid of) your devices from now on.

Provided by The Conversation