Defend all your devices from hackers

Tips include computer locks, disabling locations
If you spot an unknown location or a device that isn't yours, act fast. Change your password, be sure two-factor authentication is turned on and log all devices out of your account.

Kim Komando SPECIAL TO USA TODAY 4/9/2023

Some security steps are common knowledge. I don't need to remind you to install that latest update on your computer, right?

Others are less obvious. Do you lock your computer every time you get up? Unless you live alone, you should.

On your phone, you'd probably never guess leaving your Bluetooth connected 24/7 is a mistake.

I've got your back with more secrets only tech pros know to keep you safe and secure.

Check your inboxes

I always get calls to my national radio show from people concerned that someone is watching everything they do.

One of the first steps I recommend: Make sure your inbox is locked down.

Here are steps if you notice or suspect any usual logins:

Log in to your email, then go to your account or security settings. You'll find an option that allows you to view your recent login activity or login history. It will be labeled something like Recent Activity, Security or Login History. Pro tip: Use Gmail? Click the Details link next to the Last account activity at the bottom of any Gmail page. Review the list of recent logins. See anything that isn't you or one of your devices? You may see a strange location, too.

If you spot an unknown location or a device that isn't yours, act fast.

Change your password, be sure two-factor authentication is turned on and log all devices out of your account.

Defend all your devices from hackers

Check your printer

Like your computer, your printer is a goldmine for hackers. Why? Printers often store copies of the docs that have been printed.

Any cybercriminal could get copies of sensitive information, like your financial records.

Here are three signs your printer has been hacked:

Your printer starts printing blank pages or a bunch of characters.

You notice print jobs you did not initiate.

Your printer's settings have changed – and it wasn't you.

What should you do?

Unplug the printer. Press and hold its Reset button, usually on the printer's back or bottom. While holding the Reset button, plug the printer back in and turn it on. In about 20 seconds, lights will flash to indicate it's done.

Check your phone

I recommend you look through the location settings on your phone.

That will go a long way in shutting down a lot of the GPS tracking. But you can't stop there.

Why does your phone tell you how long it'll take to get to the office or knows your ETA to the grocery store when you get in the car for Saturday morning errands?

That's part of Significant Locations.

Apple says this feature exists so your phone can learn places significant to you and provide personalized services, like traffic routing and better Photos Memories.

Here's how to access it – and shut it down:

Open your iPhone's settings, then tap Privacy & Security. Select Location Services. Scroll down and tap System Services. Scroll until you see Significant Locations and tap that.

Defend all your devices from hackers

If you don't want your iPhone to keep track of your whereabouts, slide the toggle next to Significant Locations to the left to disable the setting.

Wipe your phone if you lose it

The very idea of your phone in someone else's hands is creepy. Imagine a stranger rifling through your photos, videos, apps, conversations and browser tabs.

So what if your phone goes missing? You can take a step to protect your info, even if you never get that phone back.

To remotely erase your iPhone:

Open iCloud.com/find and go to the Find iPhone feature. Select your lost phone, then select Erase iPhone.

To remotely erase your Android phone:

Go to android.com/find and sign in to your Google account. Select your lost phone, and you'll get information on its location. When prompted, select Enable lock & erase.

Select Erase device to wipe its data.

Turn off app location trackers

Social media companies are dying to get their hands on your contacts' birthdays, pictures, full names, email addresses and more. They tell you it's a handy tool to find your friends, but your friends' info isn't yours to give away. That's their own to decide where to share.

From your address book, companies build so-called Shadow Profiles. They can learn a ton from those you know, even if they're not using those platforms. Sneaky stuff.

How can you make a difference? Don't give apps access to your phone's contacts. Review which apps do have access and turn it off. And always pay attention and stop sharing info without a real benefit to you.

Even your phone number is powerful in the wrong hands.