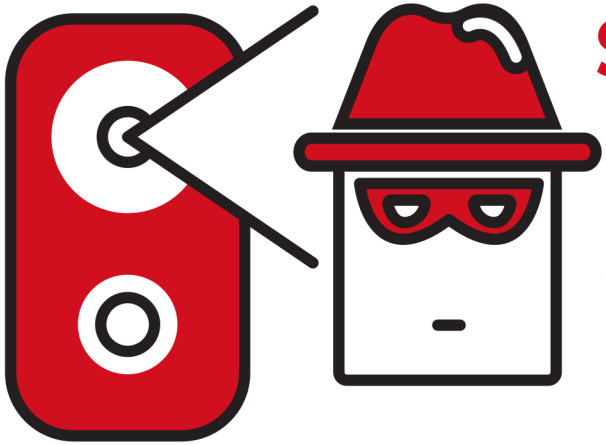
SIMPLE STEPS TO SECURE YOUR

DIGITAL DEVICES

AT HOME



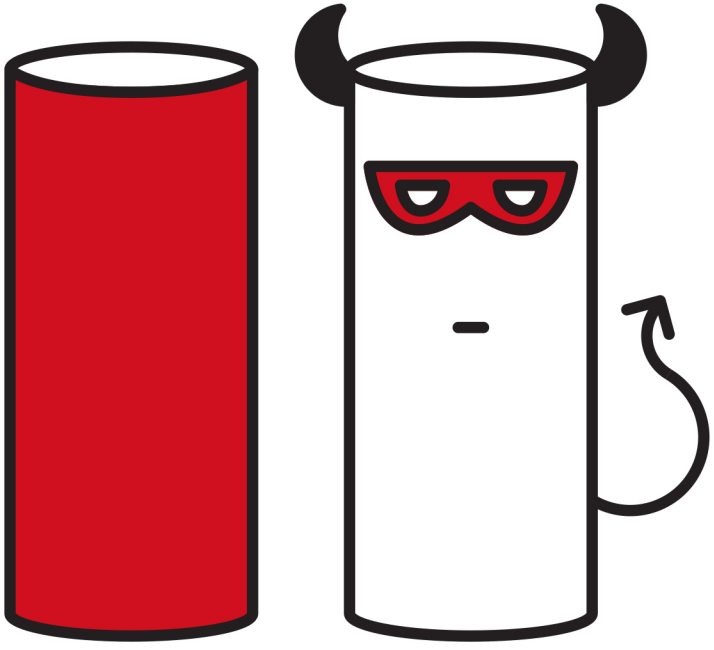
SURVEIL YOUR VIDEO DOORBELL

47% of all vulnerable devices on home networks include cameras.

After testing 11 brands, a watchdog group found the most common device flaws were weak password policies and lack of data encryption.

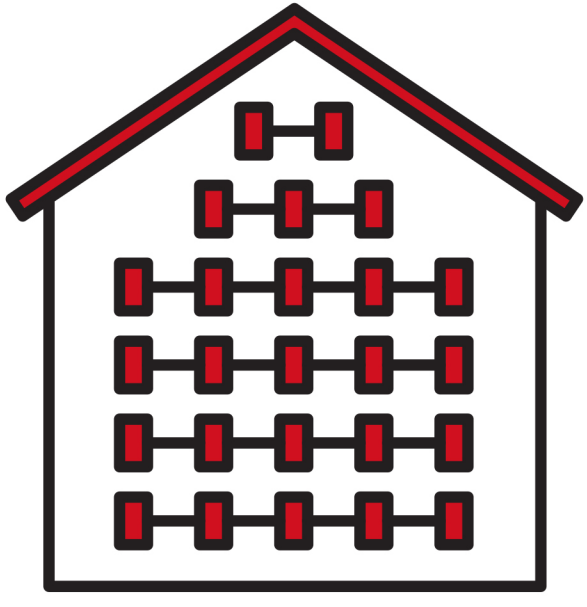
With a smart doorbell, which includes a camera and oftentimes a microphone, you can see who's at your front door right from your phone screen.

This modern gadget is useful, but without the property security settings, unwanted guests can log into your home Wi-Fi network and manipulate the doorbell's settings. To ward off hackers, update your doorbell's passcode often and enable two-factor authentication during the setup process.



BEWARE OF ALEXA'S EVIL TWIN

The average U.S. household owns 25 connected devices.

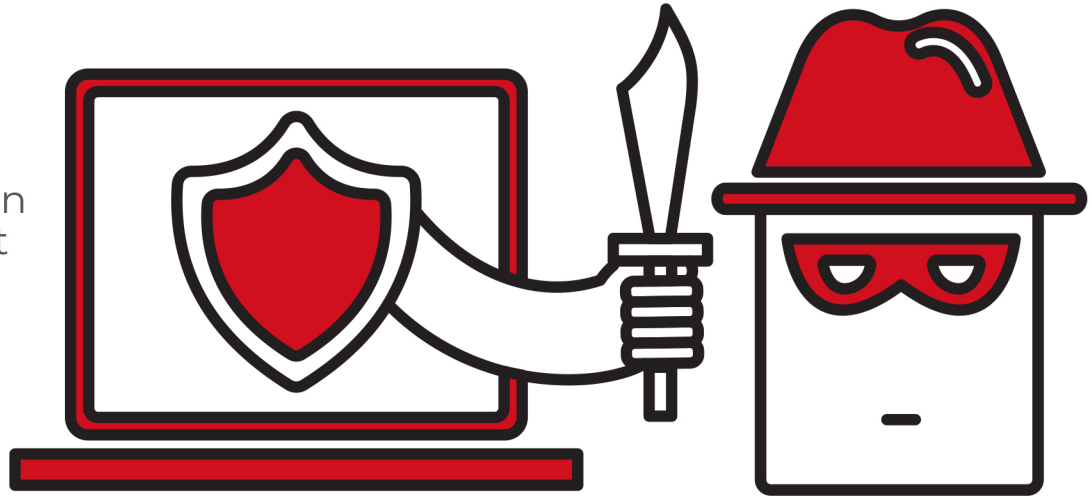


It's possible for your virtual assistant devices – like Amazon Echo (Alexa) and Google Home – to get hacked! Hackers can eavesdrop on private household conversations.

Limit the amount of information you share with your virtual assistant and decrease the number of apps connected to the service.

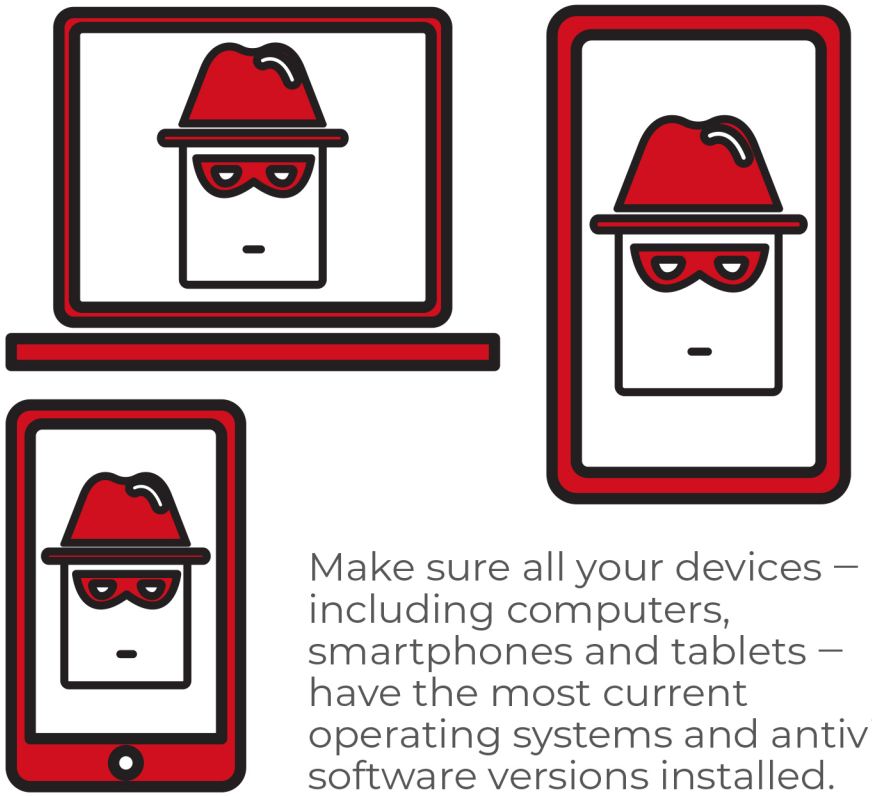
ANTIVIRUS SOFTWARE DOESN'T FULLY PREVENT ALL CYBER THREATS

Antivirus software programs can only protect against known attacks. It's important to update your software as soon as the latest version becomes available.



Only 49% of computer users have an antivirus app installed.

UPDATE YOUR DEVICES



Make sure all your devices – including computers, smartphones and tablets – have the most current operating systems and antivirus software versions installed.

80% of people who have experienced a data breach could have prevented it by updating their device's software.