October is cyber security awareness month and I'm going to kick things off with a look at the question: "can apps I don't use track me?" We've probably all downloaded a free silly game or app that we play a couple of times then forget about. Does it pose a threat? What could it do? Should you remove it?

TRT 1:27
STD OUT

supers:

9-18 Russ Schaefer/National Cyber Security Alliance
110-120 Jamey Tucker

**ANCHOR INTRO**

A FEW YEARS AGO CYBER SECURITY WAS SOMETHING FOR HOLLYWOOD TO PUT INTO MOVIES. TODAY THOUGH, IT'S PART OF OUR EVERYDAY LIVES.

FROM THE APPS WE USE TO HOME SECURITY SYSTEMS TO OUR PERSONAL WIFI NETWORK, HACKERS CAN EXPLOIT ANYTHING TO SNOOP OR STEAL IDENTITIES. OCTOBER IS CYBER SECURITY AWARENESS MONTH AND OUR CONSUMER TECHNOLOGY REPORTER JAMEY TUCKER TAKES A LOOK AT ONE THING WE ALL DO THAT PUTS OUR INFORMATION AT RISK.

**PACKAGE**

We don't think twice about downloading a free app. We'll put up with a few pop-up ads if it means we can play a game for free, or use special filters for photos. You use them a few times, have some fun and then a couple of days or weeks later...

"You've forgotten about them completely. But they're sitting on your phone collecting data, sharing data, maybe sharing location and you haven't given it a second thought."

Russ Schaefer, executive director of the National Cyber Security Alliance, says apps can do all sorts of things, but stealing your information? not technically.

"The short answer is you probably gave it permission."

Permission for what? I checked several featured apps in iTunes. They all collect first and last name, home address, email address, phone number and identifiers. Many apps in the Google Play Store are worse.

Last year, hundreds of fake apps were uploaded to the Google Play Store and were downloaded over 4 million times. Once installed, hackers gained access to texts, calls, passwords and could use the camera lens.

Schaefer says, if you're not using an app, you don't want it on your phone.

"Go through, clean out your machine. Get rid of those apps. Close them off and strip down your phone just to what you need at a time."

If you've signed up to use an app with your Facebook login, you're giving up even more information about yourself. These apps can see your profile, what you like, who your friends are, your address, phone number and your friends. So it's a good idea to go through and delete those apps as well.
That's What the Tech? I'm Jamey Tucker

**ANCHOR TAG**

APPS COLLECT INFORMATION ON ANYONE WHO INSTALLS THEM, WHICH IS PARTICULARLY TROUBLING FOR CHILDREN. LAST YEAR, OVER ONE MILLION CHILDREN WERE VICTIMS OF IDENTITY THEFT OR FRAUD.

**WEB STORY**

We don't think twice about downloading a free app. We'll put up with a few pop-up ads if it means we can play a game for free, or use special filters for photos. You use them a few times, have some fun and then a couple of days or weeks later...

"You've forgotten about them completely," said Russ Schaefer, executive director of the National Cyber Security Alliance. "But they're sitting on your phone collecting data, sharing data, maybe sharing location and you haven't given it a second thought."

Apps you download and install can, and often do, capture loads of personal information. That includes names, addresses, what websites you visit and often your GPS location. Schaefer stops short of saying the apps "steal that data."

"The short answer is you probably gave it permission. They had a privacy policy that was 25 screens long and started out by saying 'your privacy is important to us.' And buried someplace on a certain screen that says 'in the meantime to improve your experience we're going to track your location, we're going to track your browsing habits, we're going to find out information about you and build a profile to better serve you."

What's even more concerning is that some apps do steal information they don't make clear is being gathered. Especially Android apps. Last year, hundreds of fake apps were uploaded to the Google Play Store and were downloaded over 4 million times. Once installed, hackers gained access to texts, calls, passwords and could use the camera lens.

If you've signed up to use an app with your Facebook login, you're giving up even more information about yourself. These apps can see your profile, what you like, who your friends are and, if you've entered it into Facebook, your physical address, email address, phone number and birthdate. That's enough information for a hacker to get a start on stealing your identity and selling the information on the dark web.

The latest Facebook data breach, announced last week, might have also allowed hackers to access and use your accounts for the apps you've signed up for with your Facebook login.

Schaefer says, if you're not using an app, you don't want it on your phone.

"Go through, clean out your machine. Get rid of those apps. Close them off and strip down your phone just to what you need at a time."

This is especially important for children who download apps and sign up using an address or phone number. It gives the bad guys a start on gathering enough data to begin working on stealing their identity. Last year, according to the National Cyber Security Alliance, more than 1 million children were victims of identity theft or fraud.

Parents, know what you're kids are downloading and warn them about what information they're giving away...in order to play a silly free game.