Only IDIOTS Own 'SMART' Phones

Sat, 02 Dec 2023 10:02:19, swmof88, [category: news, post_tag: only-idiots-own-smart-phones]

[Professional hacker reveals the five mistakes that allow anybody to crack into your smartphone within SECONDS]

Keiran Burge, a legal hacker, tells MailOnline what five common mistakes people make that let cybercriminals access their private data and take control of their devices.

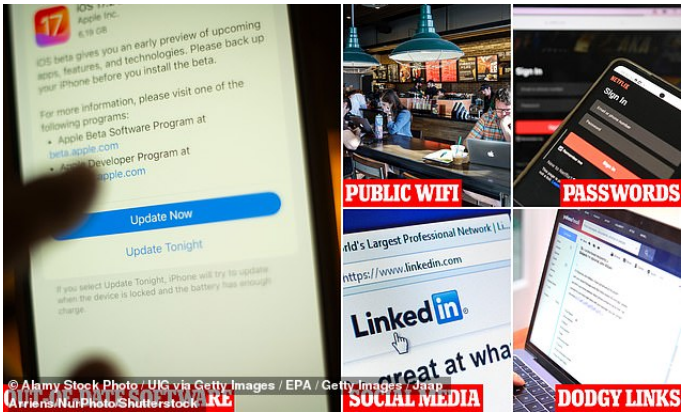
Many of us would feel lost without our smartphones in hand - but what if that same device became a tool for criminals?

Kieran Burge, a security consultant at Prism Infosec, has revealed the five common mistakes that could let him crack into your smartphone within seconds.

As a penetration tester - a legal hacker who tests companies' cybersecurity to find weaknesses before criminals do - Kieran knows what he's talking about.

And he says that simple mistakes such as reusing passwords, clicking on dodgy links and sharing too much information on social media could land you in hot water.

So, are you guilty of these security blunders? Read on to find out.



-

Kieran Burge, a security consultant at Prism Infosec, has revealed the five common mistakes that could let him crack into your smartphone within seconds

As a penetration tester - a legal hacker who tests companies' cybersecurity to find weaknesses before criminals do - Kieran knows what he's talking about

READ MORE: [Urgent warning to Mac users over fake browser updates that can steal your passwords]

1. Using out-of-date software

Keiran told MailOnline that one of the first things he and other hackers look for when preparing an attack is out-of-date software.

'Out-of-date software is a really big issue because, if the software has been updated, it's probably because there is a security issue', he explained.

Software, whether it is the operating system of your iPhone or the control system for a factory, often has some sort of vulnerability.

While these can quickly fixed by developers, they are also often shared online through forums and hacker communities.

If you haven't updated your software to include the fix, Keiran explains, 'people can get in and steal really sensitive information and even sometimes take control of the software.'

Keiran told MailOnline that one of the first things he and other hackers look for when preparing an attack is out-of-date software

What are some of the most commonly hacked passwords?

Research by Specops Software has found that easily predicted passwords are still commonly used.

Some of the most frequently compromised are:

- research
- GGGGGGGG
- Cleopatra
- Sym_cskill
- mcafeeptfcorp
- minecraft.A.S
- sym_newhireOEIE
- password

The vulnerabilities can take many different forms and allow criminals to cause serious disruption for companies and individuals.

These attacks are often opportunistic as criminal groups scan online archives for out-of-date versions of software.

Keiran says the recent crippling hack on the British Library was likely to have been an opportunistic attack of this kind

To keep safe online, Keiran says you should 'always ensure that your software is up to date.'

2. Reusing passwords

Another common way that hackers get hold of your personal data, according to Keiran, is by exploiting reused passwords.

Keiran told MailOnline: 'No matter what site you're giving information to you, you don't know what they're going to do with that information or how they're going to protect it.'

He says that the big risk of re-using passwords is that if even one site you use is compromised, it can give hackers access to all of your accounts.

'As soon as a company is breached there's usually a big database dump that gets put on the darkweb,' Keiran said.

The dark web is an encrypted part of the internet not accessible with normal search engines which is often used to host criminal marketplaces.

In April this year, an international raid brought down a hacker bazaar called Genesis Market which the FBI claims offered access to over 80 million account access credentials.

Keiran said: 'There are going to be databases out there with user name and password combinations for your accounts.'

'If you're reusing passwords then any hacker can take that combination and use it to take control of another company.'

-

Reusing passwords puts you at risk because your account credentials can be stolen and resold on marketplaces like Genesis Market which the AI took down earlier this year

3. Giving out too much information online

'On a personal level, for someone in their day-to-day activities one of the most important things that people need to think about is how much information they're sharing online,' Keiran said.

In 'red teaming' - a cybersecurity term for testing the defences of a company - one of the first places Keiran and his team look is social media.

'We can do almost anything to get into a company, but one of the tools we use is harvesting data from social media,' Keiran explained.

'We scour social media sites like LinkedIn to see what we can find.'

Not only might this reveal usernames which can be linked to stolen account credentials, but it also opens the door to a whole range of other attacks.

One of the most insidious attacks that this exposes you to is a technique called 'sim swapping' or 'sim-jacking'.

Keiran explains that hackers will search the web for information such as your date of birth, address, and even the answers to common security questions like your mother's maiden name.

'Once you have all that information you can use social engineering techniques to ring up their mobile provider and convince them to transfer the mobile number to a new sim,' he said.

Now, whenever a text or call would go to the victim's phone it instead goes straight to the attackers.

'Once they have that you suddenly have access to all the multi-factor authentication sites that the person is signed up to,' he added.

This could include work email accounts, online shopping accounts, and even online banking.

'Everything you put up online you no longer have control over, and if you're unlucky and all that information links up then you can get your identity partly stolen,' Keiran warned.

Giving away too much information online can leave you at risk of Sim-Jacking attacks in which hackers transfer your phone number to a new sim to intercept your calls and messages (stock image)

READ MORE: **I'm a hacker who was jailed for a decade for heading up a cybercriminal organization**

Jesse William McGraw, 39, spent a decade in prison for heading up one of the first cybercriminal groups in America

4. Connecting to unprotected public networks

'In the last few years something that's become a lot more important is remote working,' Keiran said.

'A big part of that involves people going to cafes like Starbucks and connecting to their public WiFi.'

The problem is that these kinds of public networks use a type of system called 'open authentication' to connect your device to the web without having to use identity verification.

While this makes it easy for you to quickly jump onto the coffee shop WiFi to send a few emails, it also puts you at risk of attacks from cybercriminals.

Open authentication means that the data you send across the network is not encrypted and can be captured by anybody else on the network.

'Someone could be sat outside a public WiFi network and just listening in on what's being sent,' Keiran warned.

'They could be in the cafe or they could be using specialist hardware to increase the range at which they can listen in on the network.

'They can be hidden a safe distance away then all they have to do is listen and wait.'

To avoid personal information like banking details being stolen from public WiFi, Keiran recommends that you always use a VPN when in public.

These services encrypt your data so that any eavesdroppers on the network won't be able to read what your sending.

-

On public WiFi anyone could be listening in on the information you're sending, waiting to steal sensitive information such as bank details and passwords

READ MORE: [ChatGPT could help scammers write perfect phishing emails]

5. Clicking dodgy links

Finally, Keiran says that sending dodgy links is still the most common way that people get hacked.

Phishing scams remain the most prevalent attack in the UK according to the UK's National Cyber Security Centre (NCSC).

In 2022 alone, 7.1 million malicious emails and URLs were flagged to the NCSC - the equivalent of nearly 20,000 reports a day.

Keiran explains that hackers will send fake emails and text messages to targets containing links to malicious websites or instructions to download software.

Once one of these links has been clicked, it gives criminals a window to install malware on their victim's device which can steal data and even take control.

But as sophisticated as a computer virus might be, hackers still need someone to follow a link

Biden And Obama Govt Use Silicon Valley To Put An Electronic Dog Leash On Every Citizen
- Never sign-in to any web site and always hide anything that could identify you on-line.

Want to help end the tech oligarch's rape of society? Never, EVER: use, read, quote, link to, paste from, or refer to; anything on corrupt and contrived: Twitter, Google - Alphabet - Facebook - Meta - Instagram - Netflix or YouTube! Don't expand their reach! Don't be their digital bitch! Stop being an addict to Silicon Valley's social media scam! Keep the battery out of your phone so Big Tech can't continue to spy on you. Did you know you CAN'T turn an iPhone off. Apple iPhone's pretend to be "off" but still monitor you with reserve power. Congress should shut these companies down, but they don't because these companies pay the largest bribes on Earth to politicians! Demand that Congress shut down these big tech abusers that cause child suicides, bullying, sex trafficking, money laundering, tax evasion, political bribery, election manipulation and other social crimes.

to a compromised website or download files containing hidden malware.

'You need to be vigilant of anyone that is sending you something when you don't expect it,' Kieran concluded.

'Don't click on dodgy links, don't download dodgy files, don't fall into their trap.'

FBIiPhone

Share or comment on this article: I'm a professional hacker - and these are the 5 things that would allow me to crack into your smartphone within SECONDS

EVERY DEVICE that SILICON VALLEY SELLS YOU, OR CONNECTS TO YOU, WILL HURT YOU AND YOUR FAMILY!

All Electronics that you have log-in to will ALWAYS eventually be hacked and spy on you and manipulate you and report you to government and political bosses.

"AI" = Spying on you, data rape, monopolistic control & political information manipulation
"Google" = Spying on you, data rape, monopolistic control & political information manipulation
"Amazon" = Spying on you, data rape, monopolistic control & political information manipulation
"Meta" = Spying on you, data rape, monopolistic control & political information manipulation
"The Cloud" = Spying on you, data rape, monopolistic control & political information manipulation

NEVER trust ANY of these things and never connect to them!

Biden And Obama Govt Use Silicon Valley To Put An Electronic Dog Leash On Every Citizen
- Never sign-in to any web site and always hide anything that could identify you on-line.

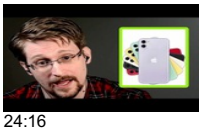
Want to help end the tech oligarch's rape of society? Never, EVER: use, read, quote, link to, paste from, or refer to; anything on corrupt and contrived: Twitter, Google - Alphabet - Facebook - Meta - Instagram - Netflix or YouTube! Don't expand their reach! Don't be their digital bitch! Stop being an addict to Silicon Valley's social media scam! Keep the battery out of your phone so Big Tech can't continue to spy on you. Did you know you CAN'T turn an iPhone off. Apple iPhone's pretend to be "off" but still monitor you with reserve power. Congress should shut these companies down, but they don't because these companies pay the largest bribes on Earth to politicians! Demand that Congress shut down these big tech abusers that cause child suicides, bullying, sex trafficking, money laundering, tax evasion, political bribery, election manipulation and other social crimes.

pixelprivacy.com › resources › spying-on-your-cell-phone

Is Someone Spying on Your Cell Phone? How to Tell & Stop Them

You use your cell phone on a daily basis, sending emails and text messages, making calls, listening to voicemail messages, taking and sharing videos and photos, using social media, and so much more. What if someone was able to access all of that personal data? That could be a disaster. Why Would Someone Spy On My Cell Phone?

Videos from your phone spies on you


24:16

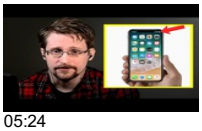
Edward Snowden: How Your Cell Phone Spies on You

YouTube

02:01

Is your phone spying on you?

YouTube


05:24

How Your Phone Is Spying On You | Edward Snowden

YouTube

16:26

Stop Your Android From SPYING On You!

YouTube

04:04

How-To Detect If Someone's Spying on Your Phone [HACKED]

YouTube

11:44

4 Smartphone Spy Hacks YOU CAN DO RIGHT NOW (Awesome Spy Apps)

YouTube

05:25

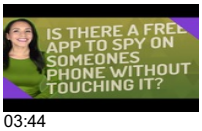
Secret phone codes can spy on you without your knowledge!

YouTube

04:32

DON'T USE MOBILE SPY APPS! (there's a good reason why)

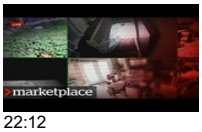
YouTube



03:44

Is there a free app to spy on someones phone without touching it?

YouTube



22:12

How hackers could use smart home devices to spy on you (Marketplace)

YouTube

See more videos from your phone spies on you.

popularmechanics.com › technology › apps › a33448364 › how-tell-apps-spying...

App Spying - How to Tell If Someone Is Spying on Your Phone

Apps could be secretly accessing your smartphone's microphone and camera to spy on you, or collect data to serve you targeted ads. To protect yourself, you can download an app that lets...

vpnoverview.com › privacy › devices › is-your-phone-being-monitored

Mobile Spyware: How to Tell If Your Phone Is Being Monitored

If your phone is constantly slowing down or lagging, this could be caused by malware. Spyware (which is a specific type of malware) operates in the background of your device and uploads your data, photos, and documents to an external server. These tasks are resource-intensive, resulting in slow performance.

rd.com › list › phone-apps-spying-on-you

If These Apps Are Still on Your Phone, Someone May Be Spying on You

CamScanner Ana Bera is a cybersecurity expert with Safe at Last. She identified CamScanner, an app meant to imitate a scanner with your phone, as one of the apps consumers should be concerned...

androidauthority.com › is-your-smartphone-spying-on-you-953309

Gary Explains: Is your smartphone spying on you?

If the keyphrase isn't heard, nothing happens. Once the keyphrase is detected, the device will send a snippet to Google's servers to double-check if it was a false positive. If everything ...

universityofcalifornia.edu › news › what-happens-when-your-phone-spying-you

This is what happens when your phone is spying on you

March 23, 2023 Ioana Patringenaru, UC San Diego Credit: David Baillot/University of California San Diego Smartphone spyware apps that allow people to spy on each other are not only hard to notice and detect, they also will easily leak the sensitive personal information they collect, says a team of computer scientists from New York and San Diego.

zdnet.com › article › how-to-tell-if-someone-using-your-iphone-to-spy-on-you

How to tell if someone is using your iPhone to spy on you (and how to ...

You can have more than one face, and set of fingerprints enrolled in your iPhone. To check if someone has added their face to Face ID, tap Settings > Face ID & Passcode and enter your passcode. If ...

nordvpn.com › blog › is-my-phone-listening-to-me

How to stop your phone listening to you [+Video] | NordVPN

It is easy to test if your phone is spying on you — simply select an unrelated topic and talk about it a few times within earshot of your phone. You can follow these steps to find out if your phone has been listening and logging your conversations: Select a good topic.

makeuseof.com › what-happens-when-phone-spies-you

What Happens When Your Phone Spies on You? - MUO

What Happens When Your Phone Spies on You? By Damir Mujezinovic Published May 4, 2023 Do you think someone is tracking your smartphone? Is it infected with spyware? Here are some red flags that indicate someone might be spying on you. Readers like you help support MUO.

today.ucsd.edu › story › spywarestudy2023

This is What Happens When Your Phone is Spying on You

Spyware apps surreptitiously run on a device, most often without the device owner's awareness. They collect a range of sensitive information such as location, texts and calls, as well as audio and video. Some apps can even stream live audio and video. All this information is delivered to an abuser via an online spyware portal.