one brightly cyber

WE MAKE CYBER SIMPLE

HAS YOUR DEVICE BEEN COMPROMISED?

Every device is at risk of compromise, desktops, home computers, mobile phones, tablets, and more.

Being concerned that your device has been compromised is healthy. After all, if it is your office computer then your credentials are at risk and with them, company and customer data, the latter requiring protection under law.

If it is a home computer, tablet, or mobile phone the risk is again your credentials but also access to your bank accounts, investment accounts, medical files and more. If the device is used for personal and business purposes, then the risk is compounded.

Is there a guaranteed way to tell if the device has been compromised? Sadly, no. But there are things that if present are a good indication of compromise. Some of these are for all devices and some are more for mobile devices.

Strange behavior is an indicator of possible compromise, and it is anything out of the ordinary for your device.

It may be slow response to commands, touch, tap, or typed. This may be due malware running on the device.

Temperature is an indicator of how hard the device is working. Does the device feel hotter than usual, especially after sitting idle? If so, then programs you are unaware of, such as malware, may be running. These programs will use CPU generating heat and reducing battery life.

Do you monitor your data usage? If so, then seeing an increase, especially a significant one may indicate malware running and sending your information back to a command server.

Do you see calls or texts that don't appear familiar to you? They may be created and sent by malware. If you don't monitor your data usage start now. Get a general sense of data usage over a day, a week, and a month. That way you can spot unusual activity.

New or unusual pop-ups are another sign of possible malware infection. Be very careful with them as it is not uncommon for cybercriminals to initiate them. Worse yet, they will make clicking on the X that usually closes the window the same as clicking on the button to select the popup or service taking you to a malware site and potentially putting more malware on your device.

Have any new apps appeared on your screens? If you don't remember putting them there, then the chances are very high they are malware. Delete them immediately.

Have any of your accounts shown unfamiliar activity? Purchases, financial transactions, large data transfers, etc? Another sign of malware.

WE MAKE CYBER SIMPLE

HAS YOUR DEVICE BEEN COMPROMISED?

An account porting attack is one of the most devious attacks. It is for mobile devices only. You may receive an email or text from your carrier about an account change. Then about 30 minutes later your phone is dead, can't send or receive data or make or receive phone calls. If this happens report it to the police immediately, then call your carrier. It means a cybercriminal has taken control of your account and had it transferred to another device that they control.

A typical approach for this type of attack is that the cybercriminal contacts your carrier and reports that they lost their phone. They have enough of your private information to convince the carrier they are the rightful owner of the account which is then transferred to a new device. Your device is dead. The burden is now on you to prove to the carrier that you are indeed the rightful owner of the account, and it isn't easy.

In this case as the old saying goes an ounce of prevention is worth a pound of cure.

Use two factor authentication for all applications on all devices. Even if it is more inconvenient.

Never use public WiFi as it is never secure.

Never click on any link you weren't expecting and even then, be cautious on what you click.

Public charging stations, especially the ones in airports have often been compromised and will download malware onto your device while charging it. Always plug your charger into an electrical outlet, never into a USB charging station.

Never leave your phone unattended. It is common to leave your phone on the table in a coffee shop when going to get a refill or use the restroom. No matter how friendly that person at the next table has been you don't know them. It is far too easy to steal the phone and leave before you return or to download malware onto the device then assure you it hasn't been touched.

Are you ready to get serious about protecting your assets and your company?

Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.