Blog Article

# Keeping Your Smartphone Safe from Hackers

Cybercrimes have been a hot issue in the news lately. There was the U.S. retailer Target, where hackers got hold of 40 million customers' debit and credit card information and at Bell, 22,000 of their small business customers had their account information compromised by a third party. In terms of individuals, hacking bank accounts has unfortunately become so common that we all know someone who has been affected by it.

Hackers are now seeing smartphones as a goldmine for retrieving sensitive private information. According to an article from WNCN, you can download phone hacking software for as little as $20. Even though it is intended for parents to monitor their children, it can easily go into the wrong hands. The Guardian wrote that a flaw in iOS software puts Apple in a vulnerable state for the hackers. Third party intercepting and stealing sensitive private information like email, bank account, text messages is a serious growing concern for everyone.

So how do hackers hack? All digital information needs to go from place A to place B. It is sent via an unintelligible code to protect it from unwanted third party interference. This practice of 'secret code' is called cryptography. Place A encrypts the information and then is decrypted when it is received by place B. Hackers try to break the encrypted code before the message gets to place B.

At the University of Waterloo, the research group Cryptography, Security and Privacy (CrySP), focuses on those issues by developing technologies and software that will help prevent a cyber attack. Dr. Urs Hengartner, Associate Professor at the David R. Cheriton School of Computer Science and CrySP faculty member, specializes in privacy and security issues in mobile social networking and location-based services. He explained that one of the methods hackers use to find information in your smartphone is through an unsecure public Wifi network. In addition, third-party apps for social networking sites or smartphones can have malware that takes your personal information. CrySP develops and creates software that helps smartphone users to continue using their apps and keep their privacy protected.

To protect your data from third parties, Hengartner recommends be judicious of what you install on your smartphone. On Google Play, for example, anyone can upload an app; validity and the safety of the apps are not always a guarantee just because an app is on Google Play. If you use an Android phone, watch what add-on permissions to allow.

It is also important to be selective on what you choose to browse on a smartphone. For example, online banking should be done on a computer browser than a smartphone as more research has been done regarding the safety of computer browsers. It is recommended that you do not put yourself at risk by using a smartphone.

Criminal hackers will continue to come up with sophisticated ways to intercept information so it's important to be conscious about keeping your smartphone and all electronic devices safe.