# SecureCrypt Secure Communications Introduces Cellular Network Protection

**SecureCrypt, a secure communications provider is now offering cellular network protection to guard against Location Tracking, IMSI Catchers and more, on top of the providers already extensive set of secure communications solutions.**

**Toronto, Ontario Apr 7, 2022 (Issuewire.com)** - SecureCrypt, a secure communications provider from Toronto, Canada is excited to announce their Cellular Network Protection Technology that includes Location Tracking Blocking, IMSI Catcher/Stingray Detection & Avoidance System, DNS Manipulation Attack Protections, APN Redirection Attack Protections, SS7 Attack Protections, Personal Threat Notifications, and much more.

There has been a gap in the secure communications industry regarding cellular network protection. SecureCrypt introducing Cellular Network Protection Technology now fills this gap, with SecureCrypt offering complete 360-degree device protection including hardware-based security features, application-based security features, and SecureCrypt's Encrypted Communication Application.

SecureCrypt has been on market since 2019 and has been offering secure phones housing a secure and locked-down version of Android using verified boot, kernel hardening, device attestation, enhanced memory protection, and more.

Within the SecureCrypt architecture sits the SecureCrypt Encrypted Communications Application which sits inside of an encrypted partition, isolated from the rest of the phone. The communications application does not request location or contact permissions, requires no email or phone number, and features encrypted instant messaging, encrypted group chat, encrypted voice calling, encrypted group calling, encrypted vault, encrypted voice messaging, and file transfer/storage fully end-to-end encrypted, both at-rest and in-transit with all metadata encrypted.

Using enhanced security features not found elsewhere like Duress Password, Remote Wipe, in-app Panic Wipe, Self Destructing Messages, and Stealth Mode, SecureCrypt has quickly become a leading secure communications provider globally. The introduction of SecureCrypt Cellular Network Protection Technology only solidifies SecureCrypt as a global leader in the secure communications space.

Telecoms and malicious state or non-state actors can easily track your location even with a secure phone. SecureCrypt can now prevent any global telecom from tracking your location on the cellular network with their industry-first, complete mobile threat protection including the SecureCrypt Encrypted Communications Application which prevents any electronic eavesdropping or interception of mobile communications.

SecureCrypt Cellular Network Protection Technology doesn't just focus on the phone's IMSI. Their phones come with multiple IMSIs, multiple IMEIs, and multiple Mobile Network Identities (PLMNs). With multiple cellular network identities, and the ability to swap out serial numbers on the cellular network, your phone can always suddenly appear as a different phone if an attack is ever attempted.

SecureCrypt Cellular Network Protection Technology also protects against DNS Manipulation Attacks, APN Protection Attacks, Denial of Service Attacks, Mobile Impersonation Attacks, Malware/Trojan Injection Attacks, SS7 Attacks, Diameter Protocol Attacks, and more. SecureCrypt can also offer per device DNS Cache and Data Firewall Rules as well as personal notifications when any Location

Tracking request or attack attempt has been made on your phone.

SecureCrypt also offers firmware/hardware-based protections like disabling sensitive sensors used for tracking such as GPS, Bluetooth, Wi-Fi, and NFC sensors. This combined with SecureCrypt Cellular Network Protection Technology and the SecureCrypt Encrypted Communications Application offers best-in-class protection for anyone who needs to secure their sensitive communications.

With nation-state level espionage, telecom complicity, and spying by foreign governments over a weak and outdated international telecommunications infrastructure it has never been more imperative to approach communications privacy from a position of high security with 360-degree defense.

SecureCrypt's live and dynamic IMSI Catcher Detection & Avoidance System works seamlessly in the background to be always-on. If any IMSI Catcher is detected, your phone will automatically and momentarily disconnect from the cellular network, assign itself a new and clean IMSI, IMEI, and PLMN, and reconnect to the cellular network appearing to be a new, and different phone.

A SecureCrypt blog post goes in-depth into the threat of IMSI Catchers, and explains that recently IMSI Catchers have been found outside of international embassies globally, placed by malicious foreign intelligence actors and criminal organizations.

If you are an embassy, Consul, or any government entity operating both domestically or internationally in foreign territory, SecureCrypt's enhanced privacy phones can stop any foreign government, malicious actor, or state-sponsored threat from tracking your assets on the ground, keeping them safe.

SecureCrypt's SOC Analysts (Special Operations Centre Analysts) are actively monitoring and proactively managing any live threats to clients. With their live and always-on threat management system, their SOC Analysts receive live second-by-second threat reports as they occur. If there are any Location Tracking attempts, IMSI Catcher/Stingray Attacks, Man-in-The-Middle Attacks, DNS Manipulation Attacks, APN Redirection Attacks, Denial of Service Attacks, or Malware/Trojan Injection Attacks of any kind attempted against any client phones, SecureCrypt Cellular Network Protection Technology immediately stops any attack, dead in its tracks. There is no intervention required.

With No Server Storage of any kind, and all encryption keys created on the device by the user, SecureCrypt was built so that nobody has access to your private information, not even SecureCrypt as a provider. Zero-Trust is at the core of their belief system. SecureCrypt uses quantum-resistant, intelligence agency grade 512-bit ECC (Elliptic Curve Cryptography) in the SecureCrypt Encrypted Communications Application to assure clients' privacy

SecureCrypt was designed for lawyers, activists, journalists, government, finance, NGOs, celebrities, security contractors, privacy enthusiasts, and anyone seeking true mobile privacy. With their device level, hardware/firmware level, application level, and network-level protections, SecureCrypt's 360-degree complete suite of privacy-based protections will suit anyone seeking a higher level of security. SecureCrypt hardware-based protections make SecureCrypt FIPS 140-2 compliant.

**Media Contact**

SecureCrypt

info@securecrypt.ca

Source : SecureCrypt

See on IssueWire