The Next Generation of Hacker-Proof Technology Has Arrived!

Sun, 23 Feb 2014 16:00:00, newstips66, [post_tag: blackphone, post_tag: dark-mail, post_tag: democri-c, post_tag: hacker-prooof, category: idea-theft, post_tag: vello, post_tag: viber, category: worldnews]

The Next Generation of Hacker-Proof Technology Has Arrived!

http://www.youtube.com/watch?v=qAT_ina93NY

http://www.youtube.com/watch?v=_YffwdsnKXo

A variety of hardware and software is now on the market to keep hackers out of your life and protect your privacy. The most important thing, with each, is to configure the security settings on them properly or hackers will just be using them to listen in on you or misdirect you to the wrong information. Set them up properly and you will have less spam, less personal data abuse and better security. They include:

##

TOR- https://www.torproject.org/about/overview.html.en

Tor: Overview

Topics

Inception

Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the U.S. Naval Research Laboratory. It was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications. Today, it is used every day for a wide variety of purposes by normal people, the military, journalists, law enforcement officers, activists, and many others.

Overview

Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.

Individuals use Tor to keep websites from tracking them and their family members, or to connect to news sites, instant messaging services, or the like when these are blocked by their local Internet providers. Tor's hidden services let users publish web sites and other services without needing to reveal the location of the site. Individuals also use Tor for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses.

Journalists use Tor to communicate more safely with whistleblowers and dissidents. Non-governmental organizations (NGOs) use Tor to allow their workers to connect to their home website while they're in a foreign country, without notifying everybody nearby that they're working with that organization.

Groups such as Indymedia recommend Tor for safeguarding their members' online privacy and security. Activist groups like the Electronic Frontier Foundation (EFF) recommend Tor as a mechanism for maintaining civil liberties online. Corporations use Tor as a safe way to conduct competitive analysis, and to protect sensitive procurement patterns from eavesdroppers. They also use it to replace traditional VPNs, which reveal the exact amount and timing of communication. Which locations have employees working late? Which locations have employees consulting job-hunting websites? Which research divisions are communicating with the company's patent lawyers?

A branch of the U.S. Navy uses Tor for open source intelligence gathering, and one of its teams used Tor while deployed in the Middle East recently. Law enforcement uses Tor for visiting or surveilling web sites without leaving government IP addresses in their web logs, and for security during sting operations.

The variety of people who use Tor is actually part of what makes it so secure. Tor hides you among the other users on the network, so the more populous and diverse the user base for Tor is, the more your anonymity will be protected.

Why we need Tor

Using Tor protects you against a common form of Internet surveillance known as "traffic analysis." Traffic analysis can be used to infer who is talking to whom over a public network. Knowing the source and destination of your Internet traffic allows others to track your behavior and interests. This can impact your checkbook if, for example, an e-commerce site uses price discrimination based on your country or institution of origin. It can even threaten your job and physical safety by revealing who and where you are. For example, if you're travelling abroad and you connect to your employer's computers to check or send mail, you can inadvertently reveal your national origin and professional affiliation to anyone observing the network, even if the connection is encrypted.

How does traffic analysis work? Internet data packets have two parts: a data payload and a header used for routing. The data payload is whatever is being sent, whether that's an email message, a web page, or an audio file. Even if you encrypt the data payload of your communications, traffic analysis still reveals a great deal about what you're doing and, possibly, what you're saying. That's because it focuses on the header, which discloses source, destination, size, timing, and so on.

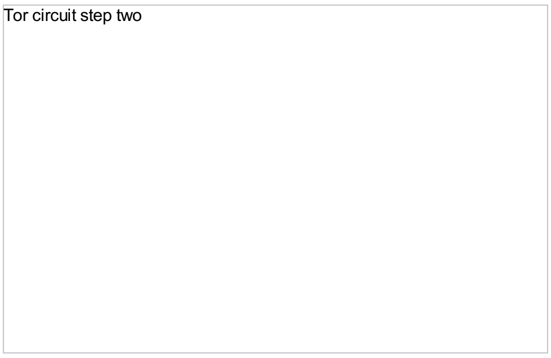
A basic problem for the privacy minded is that the recipient of your communications can see that you sent it by looking at headers. So can authorized intermediaries like Internet service providers, and sometimes unauthorized intermediaries as well. A very simple form of traffic analysis might involve sitting somewhere between sender and recipient on the network, looking at headers.

But there are also more powerful kinds of traffic analysis. Some attackers spy on multiple parts of the Internet and use sophisticated statistical techniques to track the communications patterns of many different organizations and individuals. Encryption does not help against these attackers, since it only hides the content of Internet traffic, not the headers.

The solution: a distributed, anonymous network

Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination. The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you — and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going.

To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.



Once a circuit has been established, many kinds of data can be exchanged and several different sorts of software applications can be deployed over the Tor network. Because each relay sees no more than one hop in the circuit, neither an eavesdropper nor a compromised relay can use traffic analysis to link the connection's source and destination. Tor only works for TCP streams and can be used by any application with SOCKS support.

For efficiency, the Tor software uses the same circuit for connections that happen within the same ten minutes or so. Later requests are given a new circuit, to keep people from linking your earlier actions to the new ones.

Hidden services

Tor also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing or an instant messaging server. Using Tor "rendezvous points," other Tor users can connect to these hidden services, each without knowing the other's network identity. This hidden service functionality could allow Tor users to set up a website where people publish material without worrying about censorship. Nobody would be able to determine who was offering the site, and nobody who offered the site would know who was posting to it. Learn more about configuring hidden services and how the hidden service protocol works.

Staying anonymous

Tor can't solve all anonymity problems. It focuses only on protecting the transport of data. You need to use protocol-specific support software if you don't want the sites you visit to see your identifying information. For example, you can use the Tor Browser Bundle while browsing the web to withhold some information about your computer's configuration.

Also, to protect your anonymity, be smart. Don't provide your name or other revealing information in web forms. Be aware that, like all anonymizing networks that are fast enough for web browsing, Tor does not provide protection against end-to-end timing attacks: If your attacker can watch the traffic coming out of your computer, and also the traffic arriving at your chosen destination, he can use statistical analysis to discover that they are part of the same circuit.

The future of Tor

Providing a usable anonymizing network on the Internet today is an ongoing challenge. We want software that meets users' needs. We also want to keep the network up and running in a way that handles as many users as possible. Security and usability don't have to be at odds: As Tor's usability increases, it will attract more users, which will increase the possible sources and destinations of each communication, thus increasing security for everyone. We're making progress, but we need your help. Please consider running a relay or volunteering as a developer.

Ongoing trends in law, policy, and technology threaten anonymity as never before, undermining our ability to speak and read freely online. These trends also undermine national security and critical infrastructure by making communication among individuals, organizations, corporations, and governments more vulnerable to analysis. Each new user and relay provides additional diversity, enhancing Tor's ability to put control over your security and privacy back into your hands.

##

BLACKPHONE- https://store.blackphone.ch/

About Blackphone

Blackphone is the first integrated smartphone from the best privacy minds in the industry.Silent Circle and Geeksphone have partnered to combine best-of-breed hardware with all the skills and experience necessary to offer PrivatOS, an Android™ based operating system without the usual compromises.

For more information please
visit: https://www.blackphone.ch

SILENT CIRCLE

120 Waterfront St, #420

Oxon Hill MD 20745

https://silentcircle.com/
###

Democri-C http://www.democri-c.com

Created by a programming team from around the world, Democri-C™ is a community service project designed to assist those who need to communicate in disaster and regime change environments when traditional communications systems have been intentionally or catastrophically interrupted. The project is dedicated to Freedom, Safety and Community and those who strive to experience those needs. National groups and regional organizations may receive custom bulk versions of the App at 80% discount upon application.

What else can I do with the App?
The sky is the limit. By using the App with third party software and hardware you can overcome any communications barrier, crisis infrastructure failure or political blockade ranging from a neighborhood to a global level. Just keep networking and meshing everyone you can into the overall network (known as HALO).

Promote the effort:
http://www.zazzle.com/democri_c
Democri-C™ App 1.2
SOFTWARE INSTRUCTIONS
Instructions Version: 2.4

GENERAL OVERVIEW:
Democri-C™ Emergency Communications App for Non-commercial Social Needs. Did a dictator just cut off all communications in your country?

Did a disaster just destroy all of your communications resources? BE READY: Put Democri-C on your device BEFORE a crisis strikes!
Democri-C
is a mobile and desktop computer software application which creates an instant communications system using technology that each person can control by
themselves. The architecture is designed to be added to by developers in order to grow the capability of the system over time.

This uninterruptable-network App cannot be shut down by third parties and provides urgent communications, emergency and safety information in regions where extreme social conditions are placing the lives of those in the region in jeopardy and where disaster has curtailed communications. The App is only for use in non-commercial applications.

Democri-C is an accessible " lite" version of a commercial technology.
Democri-C is designed specifically to assist those in oppressive regime regions where those regimes have terminated their telephone and internet communications.

Current Modules included:
Morse code text to morse code convertor/optical broadcaster: Adjust color, speed, audio readout volume, repeat, message content.
Morse Code Training.
Cryptography/code how-to link.
Peer to Peer audio file communications: Set which devices are Team Leaders and which are Team Members (Client/Server node settings). Authorize members remotely. Send pre-recorded communications. Assign which Team Members can receive. Login security for both Team Leaders and Team
Members.
Facebook Launch.
Twitter Launch.
Updates are intended to include mesh network peer to peer Bluetooth communications, Wifi communications, use of the IR sensor on the iPhone face, routing backbones and other extensions.
If you are using this app in a hostile political environment, please study the codes and cryptographic link as indicated on Wikipedia for your
safety.

OPTICAL COMMUNICATOR:
TAP on the OPTICAL COMMUNICATOR button.
TAP into the top window and the keyboard will appear.
Type your message.
Choose what color your screen will flash. Choose a color based on either best visibility or best secrecy, depending on your situation.
Adjust the speed of the relay of the data by sliding the control in front of the little running person icon.
Adjust the volume with the volume slider. Turn the sound off if you are in a hostile location.
Turn the REPEAT function on (the circular icon) by sliding the REPEAT button on or off.
Click PLAY and aim your screen at your target.

TAP the screen to halt the optical transmission.

MESH COMMUNICATOR:
TAP on the MESH COMMUNICATOR button.
If you are in charge of a group, a family, a team, a block, a region, a pre-organized section, a floor or any other group select:
PEEPMASTER/Team Leader
If you are a member of one of those groups select:
PEEPPEER/Team Member
In each case, create a login name when the keyboard appears. If you are in a hostile region, decide, in advance, what names you will use. This can be part of your protection code system. You can change your login name each time but your PEEPMASTER/Team Leader needs to know what it is or that person cannot authorize you.
The PEEPMASTER/Team Leader node has pre-existing emergency voice commands that exist on the web. These commands do not exist on the senders phone and they each come from different servers or in segments of parts, each from different servers.
Besides the security advantage of this, this aspect ties to future embodiments of the application.
The PEEPMASTER/Team Leader node will see Team Members or PEEPPEER/Team Member's appear in a row on the right side of their control screen. Tap and highlight one of the Team Members and then tap on one of the existing emergency messages, and you can send that message to that Team Member.
So, to review: You need to have someone else with the App logged in as Team Member on another iPhone on the same network, wifi system or carrier.
The Team Leader logs in and waits for the desktop to appear on their iPhone.
A Team Member on another iPhone logs in on their iPhone as a Team Member.
After that Team Member logs in their login name will appear as a button on the right side of the Team Leaders desktop.
The Team Leader can then tap the Team Member button that appears and it will turn blue show that they are authorized for communication.
Then the Team Leader can tap any of the pre-set media files and the assigned file will be relayed to the Team Member from a remote location, (not from the Team Leaders phone in order to preserve bandwidth and reduce location finding by the bad guys) the pre-set audio file will turn blue after you tap it to show that it has been relayed to the Team Member.
The Team Leader will not hear anything. Only the Team Member that the message is sent to will hear the audio. The Team Member should have audio enabled, volume turned up or earphones in.
This communications module will operate over WiFi-only, as well as cell phone, as long as other Team Members can connect to the same WiFi network. See THIRD PARTY HARDWARE links, below, regarding extending WiFi range to 30 miles, or farther.
These range extensions can overlap and create an extensive system with the support of

others in your network. Future upgrades to the software will enhance this capability.
In villages under attack, some have connected neighbor-to-neighbor in order to relay communications.

HOW TO USE MORSE CODE:
Use the Morse Code Instruction button in the App or visit:
http://en.wikipedia.org/wiki/Morse_code

HOW TO USE CRYPTOGRAPHIC CODES:
Use the Codes Instructions in the App or visit:
http://en.wikipedia.org/wiki/Substitution_cipher
http://en.wikipedia.org/wiki/Cipher
http://en.wikipedia.org/wiki/Cryptography

THIRD PARTY SOFTWARE:
There are third party camera Apps which can zoom in on the light-casting/Morse code screen of other mobile devices communicating with you so you can record the visible Morse code and transpose it later.

THIRD PARTY HARDWARE:
If all cellular phone systems are likely to fail, peer to peer WiFi broadcast can be extended up to 30 miles per user with Bullet2™ & Ubiquiti™ point-to-point systems, Nanostation Loco's™, Open-mesh wireless™, Yagi optimized antennas, Connect Distant and other wireless support hardware available at http://www.cyberguys.com, http://www.amazon.com, and similar suppliers. Using these systems in series you can cover an entire city or an entire country when deployed in clever ways.
###

ZELLO -

Patrick Tucker 9:31 AM ET

This Is the App That's Fueling the Uprising in Venezuela

Entrepreneur Bill Moore was in his Austin, Texas, office last Thursday, watching explosive growth for his company's walkie-talkie app, Zello, inside Venezuela. Zello had become the favorite app of protest organizers there after recently hitting the mark as the most popular app in Ukraine. Over the past few days in Venezuela, the protests ballooned following rapidly rising food prices, controversy over President Nicolas Maduro's economic policies, public dissatisfaction over crime and multiple other factors.

Moore was finding that in Venezuela that popularity had a price. Shortly after 9 p.m., his Twitter feed blew up with messages from users inside the country. The government-owned

Internet service provider, CANTV, which hosts 90 percent of Venezuela's Internet traffic, was blocking the app as well as access to Zello's website. Downloads were dropping off considerably.

Author

Patrick Tucker is technology editor for Defense One. He's also the author of The Naked Future: What Happens in a World That Anticipates Your Every Move? (Current, 2014). Previously, Tucker was deputy editor for The Futurist, where he served for nine years. Tucker's writing on emerging technology ... Full Bio

Zello sent out the following Tweet: "If you are in Venezuela and familiar with network diagnostics tools, please respond, we need your help to understand the block applied."

> If you are in Venezuela and familiar with network diagnostics tools, please respond, we need your help to understand the block applied.
>
> — Zello Inc (@Zello) February 21, 2014

As Moore describes it, the response, like the protests themselves, was immediate and enormous. People inside Venezuela and many more from around the world wrote in with advice. Moore, Alexey Gavrilov, Zello's co-founder and chief technical officer, and the company's programmers worked feverishly through the night on a new version of the app to get around the CANTV blockade. "This was the most important thing in the company," Moore told *Defense One*. "We said, 'How do we get this done?'"

Finally, at about 5 p.m. the following day, an updated version was ready to go. The company released this tweet: "Android users in Venezuela, who cannot access the app. Please try this version and report back results."

> Android users in Venezuela, who cannot access the app. Please try this version and report back results http://t.co/e5XZKYusOw
>
> — Zello Inc (@Zello) February 22, 2014

Despite the efforts of the Maduro government, protests in Venezuela are continuing and so are downloads of Zello, one fueling the other. It's a cycle that's reminiscent of the very early days of the Arab Spring in 2010 and 2011, in which students and other protestors used social networks like Twitter and Facebook to help organize, promote and communicate through protests, eventually forcing the ouster of nondemocratic governments in places like Tunisia and Egypt.

The lesson from the events in Tunisia in particular seemed to be that when you combine an educated student class with the power of social networks and press the return key, the outcome can be democracy. But when the machine malfunctions, the result can look like a protracted war with the potential to embroil U.S. forces. The protests in Libya, in contrast, resulted in a civil war costing more than $1 billion to the U.S. and NATO. When the machine breaks down completely, the result looks like Syria, or possibly Iran, where the regime has been extremely successful shutting the opposition out of the Internet.

To Moore, Venezuela looks like digital trench warfare with governments working feverishly to outmaneuver software makers and vice versa.

Founded in Austin in 2011, Zello allows individuals to communicate to one another walkie-talkie style via a simple broadband connection. The app interface looks a like button on your phone. You press it to speak to people on a particular channel. The channels can be as small as two people or as big as hundreds of thousands. The largest in Venezuela is about 450,000, but only 600 can be active on a channel at one time, Moore said. The feel of the app is similar to the now defunct Nextel push-to-talk service, which was shut down last summer. Zello is free for individuals but companies can purchase a plan to allow more users on a single channel for $10 a month.

Zello has been downloaded some 50 million times. In addition to playing a big role in the recent Ukraine protests, it was also extremely popular during last year's unrest in Turkey.

Moore never imagined that what he was making could become a politically destabilizing force. He knew only that he wanted to make a social network around the idea of Internet-based radio. "The human voice carries so much more information than typing. We knew that was the basis of something great. If you listen to these channels you realize that it's a way for people to make friends. The surprise was that that it exploded in Turkey almost a year ago to become the number one app in Turkey around the issues that they had, and then in Venezuela."

In emails, multiple protestors said that they saw Zello as an essential tool for coordinating movement, collecting intelligence on the location of government forces, and organizing responses. In other words, Zello has clear military potential. The company reports that it has received interest from the U.S. National Guard and the U.S. United States Army Reserve Command

But Zello, which has been

downloaded more than 600,000 times in Venezuela in just a few days, has seen multiple uses, some of these extend beyond calling for marches and launching maneuvers to evade the authorities. They include organizing *guarimbas*, blockades of burning trash, to thwart National Guard and police movements. The erection of the *guarimbas* represents a clear escalation in protestor tactics away from simple peaceful marches and some report that the blockades have contributed to the casualty count, which officially hit 11 over the weekend. The use of *guarimbas*is controversial among the protestors and has been met with extremely harsh responses from troops as demonstrated in this video.

The openness of the Zello platform explains why it’s become so useful across Venezuela, but this ease of use has also led to a digital fog of war with confusion about who is using the network for what purpose. According to protestors, the government and government-supporting militia groups, or *colectivos*, will listen in on protestor channels on Zello to get information about upcoming movements or marches, distribute disinformation, or learn the identities of people on the other side. This has led to calls from protestor groups on Twitter to abandon use of the walkie-talkie app.

> #URGENTE: NO ES RECOMENDABLE USAR #ZELLO | @VOZ_URBE ¡DIFUNDIR! #ResistenciaVzla +INFO EN -> http://t.co/sJrhAvORCV … pic.twitter.com/oPGVh2sxb0
>
> — #UltimaHora (@VENSomosTodos) February 19, 2014

Moore, who says his company has no direct stake in Venezuelan politics, said there’s a simple fix to these problems: the platform allows users to create one-way communication channels, multiple communication channels, or closed channels where users must be granted to access to join. It can work like a giant open microphone, a conference call, or a radio-station.

Abelardo Jesus Marquez, a Venezuelan technology consultant and blogger sympathetic to the protest movement, said in an email that part of the problem was that too many Zello users were simply unaware of the most secure and effective ways to use the service. “The logical question would be, why [don’t] they use closed channels protected by passwords? They ignore the security implications.”

The confusion among protestors using the app as well as the government shutdown of Zello and the company’s quick response, speak to the fact that digital revolution is more complicated in Venezuela today than it was in Tunisia in 2011.

"During the Arab spring we saw the power of social media to organize people around freedom. Governments have caught on to understand that their ability to restrict this information is important. These governments will continue to restrict these [services]," said Ryan Dochuk, founder of a Toronto-based company called TunnelBear that offers Internet encryption services. Dochuk said TunnelBear has seen an enormous uptick in usage in Venezuela in the last few days, primarily through Twitter.

TunnelBear's encryption service hides the way the user is accessing the Internet, what websites he or she is visiting and what is being downloaded. It offers what's called a virtual private network, or VPN, within a larger Internet service provider. (Another example is TOR.) When a VPN is working, it functions as an invisibility cloak. In Venezuela, it's allowing people to access banned Web sites and apps, such as Zello.

TunnelBear offers a free service for moderate data usage and two other plans for more heavy usage. In response to user demand, the company has made TunnelBear completely free inside Venezuela.

> @fbajak @Zello TunnelBear should unblock Zello for iPhone and Android. We are currently providing free service to #Venezuela #censura
>
> — TunnelBear (@theTunnelBear) February 21, 2014

The decision was not an easy one. "When you decide to open up your network for free, there's financial decisions at play. There's emotional decisions at play. You open your inbox on a Friday morning and you see dozens of stories of people requiring assistance," Dochuk said. "We'll support these efforts where we can, but it's by no means full proof."

Dochuk, like Moore, has no direct interest in Venezuelan politics. But he's opposed to censorship on principle. And TunnelBear already had a lot of users in Venezuela. When he heard that the government was trying block Internet access, he knew that he had to make the service free where it was needed most. But the company would really prefer not to get overly involved in conflict areas, and so the rising death toll in Venezuela is worrisome. Also, he knows that there's only so much an encrypted network can do. In places where government censorship operations are sophisticated, like in China, Syria or Iran, TunnelBear is non-existent. (Dochuk recommends users in these countries try TOR.)

The national security implications of app wars in conflict areas can't be understated. Whether Venezuela will follow the path of

Tunisia, Libya, Syria or Iran remains to be seen. The outcome depends on multiple factors. But one is how well different sides in the emerging conflict leverage technologies like Zello and TunnelBear to achieve their objectives. Though it sounds hyperbolic, the future of Venezuela, and U.S. involvement in that country, may depend on which side makes better use of this sort of technology in the coming days and weeks. Dochuk is guardedly optimistic.

“Technology can move much faster than these governments, and I think over time, these groups will be successful getting information and freedom out.”

##

PLUS, The following Apps are being used, hacked, modified or reconfigured to provide decentralized secure communications:

SWARMLOCAL

SERVAL Program

Commotion

Globe Internet

GIZMO 5

SIPPhone

FreedomPop

PAMP

RACCOON

Zact Wireless

Ting Wireless

AutoBahn

OUTERNET

Scratch Wireless

Viber

OoVoo

Bluetronix

Red Hook Initiative

Democracy Window

Tsunami Crisis Line

Mbit

OOMA

Bittorrent

OpenPhone

Universalis Communicus

P2PNS

TerraNet/Qualcomm

TuxPhone

Tel-App Communications

PCell

Omni Campus Project

Roofnet

Wi-Fi_Direct

NFC Protocols

DCentralPlus

CounterPath Bria

Kies

Blue-Walki

Cloud-Trax

Blue-Phone

i4Bi Project

Avalanche

Magic Jack

And many more peer to peer and decentralized systems...

Pirate Bay Founder to Launch **NSA-proof** Messenger App ...
Pirate Bay Founder to Launch **NSA-proof** Messenger App. By Ernesto; on July 10, 2013; C: 195; ... One new startup that hopes to lead the way in the **next generation** of encrypted communication tools comes from Pirate Bay founder Peter Sunde.

torrentfreak.com/pirate-bay-founder-announces-encrypted-...

Encrypted Android phone is only the beginning for Blackphone ...
Blackphone, the Swiss start-up that's launching a smartphone with **encrypted communications**, is planning a series of devices around the same idea, one of the company's co-founders said on Monday.

pcworld.com/article/2101000/blackphone-plans-more-s...

□

Encrypted - End to End **Encrypted Communications** Secure Email ...
Encrypted Secure E-Mail and FTP Solutions. End to End **Encrypted Communications**. **Encrypted**.com emails can be viewed by only recipient who has **encrypted**.com email account that makes it safe for companies/institutions to send critical information via email, without worrying about a security.

encrypted.com/index-php

□

Learn to Encrypt Your Internet **Communications** | EFF ...
Some of your web **communications** can be **encrypted** to protect against traffic sniffing. Take a look at this article to learn more about HTTPS, the most common web encryption standard, as well as other browser security and privacy tips. Email and IM.

ssd.eff.org/wire/protect/encrypt

□

What are **Encrypted Communications**? - Two Way Radio ...

Encrypted Communications. **Encrypted Communication**, how would it benefit one's business to push through success and security? Well, if you may not know by now, **Encrypted Communication** has been used since the beginning of the civilised world.

comm-spec.com/encrypted-communications-php

Silent Circle - Official Site

The world's first 3G, 4G, WiFi **encrypted** mobile, video and voice service. A custom-built network for security, simplicity and service. Get in the Circle.

silentcircle.com

Encrypted Communication - OpposingViews.com

A cell phone start-up is looking to cash in on the current government surveillance hysteria sweeping much of the western world. On Wednesday, **encrypted communications** company Silent Circle and Spanish cell phone start-up Geeksphone announced their debut product: Blackphone, an "NSA-proof

opposingviews.com/tags/encrypted-communication

Encrypted Wireless Ontario | PGP Secure Messaging

Encrypted Communications provides Security for your Wireless Mobile Devices, PC's and Data Files using cutting edge end-to-end encryption technology via cloud services as well as Management Solutions for Multiple Mobile Device Types.

encryptedontario.com