EasyPhonia

Enabling your global Communications

SECURE

CLEAR, EFFICIENT, AFFORDABLE

COMMUNICATION

WWW.EASYPHONIA.COM

MISSION & VISION

MISSION & VISION

CUTTING DOWN COMMUNICATION COSTS

We live in an increasingly hyper-connected always-on society where consumers have a need to stay connected to everyone and everything irrespective of where they are in the world. The availability of new technology and spread of smartphones, laptops, iPods, and in-dash car infotainment systems has led to a convergence of communication platforms, voice, data, the internet and multimedia being available on a single device. The rules of the game have changed.

EasyPhonia's mission is to break down the costs of voice and video links, enabling clear, efficient, convenient and secure communication,

Communication is the foundation of society, and freedom to communicate fulfills a basic human need. EasyPhonia delivers exceptional customer experience using disruptive next generation technologies at affordable prices.

EasyPhonia
Enabling your global Communications

THE RISKS

Whilst corporate executives, business leaders and IT professionals understand the need to protect the data and information, they may not understand how cybersecurity issues relate to them and may be ill-equipped to defend their entities from cyberattacks aimed at the theft of sensitive information. A survey of 4,000 company directors in Australia found only approximately half of them to be cyber literate, and co-directors were only 15% cyber literate.

Cyber espionage attacks can result in destruction, damaged reputation and stolen sensitive data, including personal and private information. Cyber attacks targeted at the government may cause military operations to fail, and can also result in lives lost due to leaked classified information.

Last year in Italy alone over 80,000 complaints of unauthorized and illicit cyber security incidents were reported. This represented a year by year growth of 85%. In the US, cyber crime already costs over $100 billion per annum.

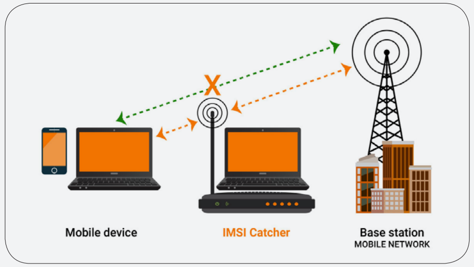
Globally, we have witnessed an increase in eavesdropping and telematic hacks. In 2017, there were over 106,000 telephone intercepts and 4,500 telematic hacks. Hackers with nothing more than your mobile phone number can listen in, record your calls, read your texts and track your location. Another common method hackers use to spread malware is through apps. They exploit mobile operating systems, non-secure Wi-Fi/URLs and firmware to replace already installed safe apps with malicious versions. Using advanced eavesdropping techniques hackers can intercept car key fob signals, break the encryption, clone the key and operate the vehicle.

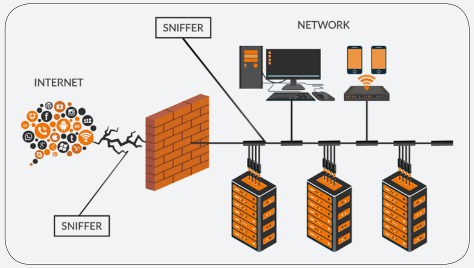
The adoption of global digital communications have made it even easier for data to cross borders resulting in an environment where an organisation's sensitive data may be transmitted and stored in servers and data centers located and managed by third parties in countries across the globe.

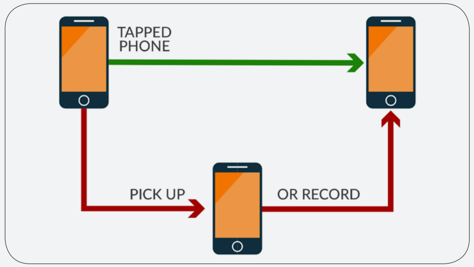
This, coupled by the rise of industrial espionage and cyber attacks aimed at infrastructures, make it virtually impossible to protect industrial intellectual property and sensitive data by installing cyber security products, and applying internal data security measures are insufficient for cross-border data protection.

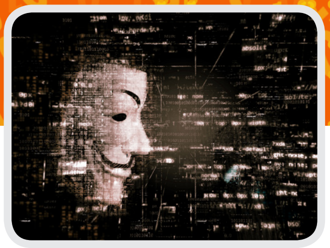
What is needed is essentially cooperation between states on cyber security to combat cross-border cyber crime, protect the entire perimeter and reduce the risks of inter-state cyber war. Bilateral cyber security agreements between states are essential to help build that cooperation.

ALL CITIZENS HAVE THE RIGHT TO PROTECTION AND CONFIDENTIALITY OF THEIR COMMUNICATIONS AND PERSONAL IDENTIFIABLE INFORMATION.









MALWARE

Malware encompasses many different types of malicious software. Malware containing viruses are software programs or code loaded onto a computer without the user's knowledge and perform unwanted actions on the computer. Worms are an invasive form of software that automatically and silently propagate without modifying software or alerting the user. After they are inside a system, they can carry out their intended harm, whether it is to damage data or relay sensitive information. A Trojan horse virus might, for example, appear to be a harmless or free online game but, when activated, is actually malware. Trojan horses appear as helpful or harmless programs but when installed carry and deliver a malicious payload. Spyware covertly gathers system information through the user's Internet connection without their knowledge. Spyware applications typically are bundled as a hidden component of freeware, shareware programs or adware that can be downloaded from the Internet. Users should know when to be concerned over application permissions and use trusted secure certificates when connecting to secure resources from the Android operating system. These certificates are encrypted on the device and may be used for Virtual Private Networks, Wi-Fi and ad-hoc networks, Microsoft Exchange servers, or other applications found in the device. These measures are necessary to ensure an adequate degree of security.

INTERCEPTION

Telephone tapping is the monitoring of telephone and Internet-based conversations by a third party. Telephone tapping often needs to be authorized by a court, and is, again in theory, normally only approved when evidence is required. The police must apply for a warrant beforehand to legally eavesdrop on conversations. Eavesdropping is normally carried out through a Telco provider. IMSI (International Mobile Subscriber Identity) Catchers are appliances freely available on the Internet for few bucks. Essentially, they are eavesdropping devices used for intercepting mobile phone traffic and tracking geolocation data related to users. They fake a legitimate cell tower between two mobile phones, and can redirect and record all traffic when no encryption tecniques are in place. These kind of sniffer attacks on signalling systems allow anyone, whether authorized or not, even with little technical expertise, to intercept communications between unencrypted mobile devices, and record timestamps, data and voice traffic.

CYBER CRIME

Cyber criminals are well-organized groups, share their exploits and tecniques, and trade data amongst themselves on the Dark Web. They use sophisticated technology, as well as industry professionals, to access personal information and sensitive corporate secrets. Social engineering attacks typically involve some form of psychological manipulation, fooling naive users or employees into handing over confidential or sensitive data, and then exploiting inadequate network security measures, vulnerabilities, and/or unpatched systems. Once hackers get this kind of information and sell it on the Dark Web, it can be used to support identity fraud, account counterfeiting, money laundering, phishing attacks or blackmail, extortion and cyber warfare. The process that stolen data goes through after the initial breach depends largely upon the type of data and from what industry it was stolen. This causes damage to a company's brand reputation, customer loss and in the worst scenario bankruptcy, (on average, about 70% of SMEs have to shut down their business after a data breach within 6 months).

WHY
EASYPHONIA

The consumer need to be “always on” and “always connected” has led to the convergence of different communication systems on a single device, whether it’s a smartphone, tablet or phablet. The rules of the game have changed. Cutting costs while allowing for clear, efficient, affordable and secure communication is Easyphonia’s mission.

The increase in connectivity requires a higher level of communication security. Protecting the confidentiality of activities related to your business cannot be underestimated and should be at the forefront of everyone’s mind, be it government, business, industry or any individual with a smartphone in their pocket. The executive, business leaders and IT professionals need to verse themselves in security threats and opportunities, to better communicate the issues and responsibilities around cyber security within their organisation, so as to secure that which needs protection with appropriate policies, procedures and tools. EasyPhonia specializes in providing secure VoIP and IP phone services to individuals, organizations and companies. Our technology allows you to configure a landline phone number in any country worldwide, on any Windows, IOS or Android device. Our EasyPhonia app allows seamless and accessible communication with your business partners and colleagues, ensuring a competitive global presence. EasyPhonia enables your global communications, offering free encrypted, secure and dynamic unlimited communications anywhere in the world. Unlimited calls forever. Unlimited and free calls for subscribers. EasyPhonia offers residential and business VoIP solutions and plans, including international calling cards.

WITH EASYPHONIA COMMUNICATION IS SIMPLE SECURE AND CONVENIENT!

WATCH THE EASYPHONIA PROJECT VIDEO
youtube.com/watch?v=BUq_dnSUtU4

SECURE LAND NUMBER ON MOBILE

Set up an encrypted local landline number directly on your smartphone, tablet or PC.

SECURE VOICE

Your phone calls with other EasyPhonia users are free and protected end-to-end with standard military encryption.

SECURE CHAT

With EasyPhonia, you can chat in complete safety with your family, friends, colleagues or whomever you wish, wherever you are.

SECURE VIDEO CALLS & CONFERENCES

EasyPhonia gives you free and protected video calls and video conferencing, even in low bandwidth environments.

VOICE TO MAIL

If an incoming call is unanswered, EasyPhonia will take the call and send you a voice message by email.

EasyPhonia
Enabling your global Communications

THE SOLUTIONS

WE'RE CONNECTED

ALL OVER THE WORLD

EasyPhonia
Enabling your global Communications
simplicity is AWESOME
wherever you are your international calls at reduced costs
CANADA
UNITED STATES
BRAZIL

ENCRYPTION

EasyPhonia end-to-end communication channel uses AES 256-bit (Advanced Encryption Standard) encryption algorithms with keys generated according to the Diffie-Hellman protocol (with support for 571-bit elliptical curve encryption) for each single phone call. These keys are destroyed immediately at the end of the phone conversation. EasyPhonia negotiates keys in peer-to-peer mode, therefore, network operators do not have access to the keys.

EasyPhonia key continuity authentication and tamper detection features enjoy self-repair properties to protect against MiTM (Man-in-the Middle) attacks.

VPN

For all users operating in regions of the world that do not allow VoIP traffic, the EasyPhonia VPN feature may be used. Easyphonia VPN will build a communications tunnel directly on its server.

EasyPhonia
Enabling your global Communications

Lookout

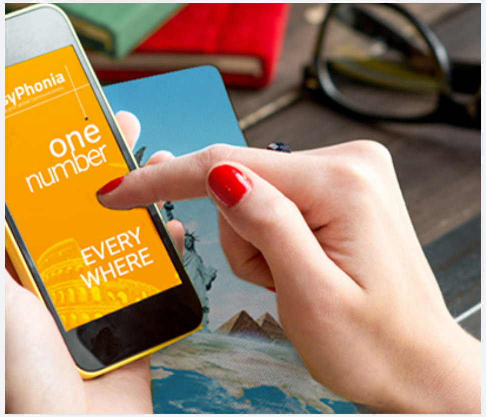
EasyPhonia uses Lookout Mobile Endpoint Security, a sophisticated rule-based EPP solution which prevents unauthorized processes during a conversation from accessing resources such as the microphone or speaker. Lookout prevents upstream or downstream listening of encrypted conversations, thus preserving privacy until the message is delivered.

EasyPhonia offers 3 packages to support users according to their specific needs.

1 **OPTION 1**
Application installed on the user's device. The EasyPhonia app is installed by the same user who will then receive the self-configuration string.

2 **OPTION 2**
Application and anti-malware. In addition to the EasyPhonia app, the user will also receive the link to download Lookout for Work, the latest generation mobile endpoint protection solution, with a set of ad hoc rules and connected to Easyphonia's Network Security Center.

3 **OPTION 3**
Phone - app - anti-malware. For users who prefer to use a different device for their conversations than they would normally use, EasyPhonia provides a 360-degree solution, also providing a next-generation mobile device (e.g. Samsung, Apple, Blackview) with the entire suite already configured.



SECURE APP

SECURE VOICE, CHAT

VIDEO CALL, VOICE MAIL

EASY**PHONIA**

+1 (302) 357-3636
+1 (302) 357-3635

EasyPhonia, LLC
501 Silverside Rd
Wilmington, DE, 19809 USA

info@easyphonia.com
www.easyphonia.com

www.easyphonia.com