How to protect yourself against Ransomware and stay safe online

Submitted by: The PR Room
Tuesday, 18 October 2016

London, 18th October 2016: Get Safe Online Day (https://www.getsafeonline.org/gsoday2016/) is the perfect opportunity to learn more about emerging online threats. Here, consumer security expert BullGuard (http://www.bullguard.com/) offers tips and advice to guard against Ransomware – perhaps the single biggest form of malware we face today.

Ransomware is a near perfect crime. Cyber fraudsters can be thousands of miles away yet lock up a computer and all its files and demand a ransom to release them, with little risk of ever being caught.

It's a low risk and high gain fraud. This is why it's spreading so quickly and why today ransomware is the most common form of malware, targeting both businesses and individuals.

Typically ransoms are in the region of £500 for individuals and several thousands of pounds for businesses.

There are many ransomware families with names such as Cryptolocker, Cerber, CryptXXX, BlackShade, Crysis, Jigsaw and the appropriately named Apocalypse. There is also ransomware that specifically targets mobile devices.

These names are a way of identifying different types of ransomware but the end result is always the same – locked files, frustration, gnashing of teeth and the need to cough up the ransom.

How to avoid becoming a victim of ransomware

• Keep an eye on the news. When a particularly virulent strain that is spreading rapidly appears, the mainstream media tends to cover it.

• Be suspicious about emails that arrive from an organisation or people you don't know, but also be vigilant about those you do. For example, strange requests from your bank to click a link to change your password, or a request to reply with personal details, should raise a red flag. Ransomware is often spread this way, and if there's any doubt contact the sender to confirm they sent the message or delete it.

• Always avoid clicking embedded links in emails that have come from a sender you don't know or have no business with. This approach is known as social engineering and is a common trick that cyber fraudsters use.

• Exercise a little caution if you find yourself being redirected to a web site that you weren't looking for. If you do find yourself on such a website don't click on any links or enter CAPTCHA codes, as this is another common way of spreading ransomware.

• Back up your important files to lessen the potential damage done by a ransomware attack. Back up on an external device and in the cloud if you are using cloud storage service such as Dropbox or Google

Drive.

• Most importantly ensure you have good layered protection on your computer such as BullGuard Internet Security. This will block dangerous websites, including harmful links, social networks and emails that are harbouring malicious code (another name for ransomware) as well as keeping you safe against other online threats.

• Ensure you regularly apply software updates whether it's to the operating system, applications or browsers. Updates are designed to patch vulnerabilities that have been discovered and cyber fraudsters will often leverage these vulnerabilities to install ransomware.

[Ends]

About BullGuard

BullGuard is Europe's number one rated consumer security company. Its award-winning product portfolio includes in-depth internet security, comprehensive mobile security, 24/7 identity protection, and social media protection for both home and small business users. BullGuard is also a pioneer in the Internet of Things (IoT) and connected device security for consumers. It released the world's first IoT vulnerability checker and following the acquisition of Dojo Labs is leading the consumer-cyber security industry in providing the highest level of protection to consumers across all of their internet-connected devices and smart homes.

More information:

Press Contact

Sarah Chard
The PR Room Ltd
Tel: +44 (0) 845 094 2902
Mobile: +44 (0) 777 9584 799
Email: sarah.chard@theprroom.co.uk