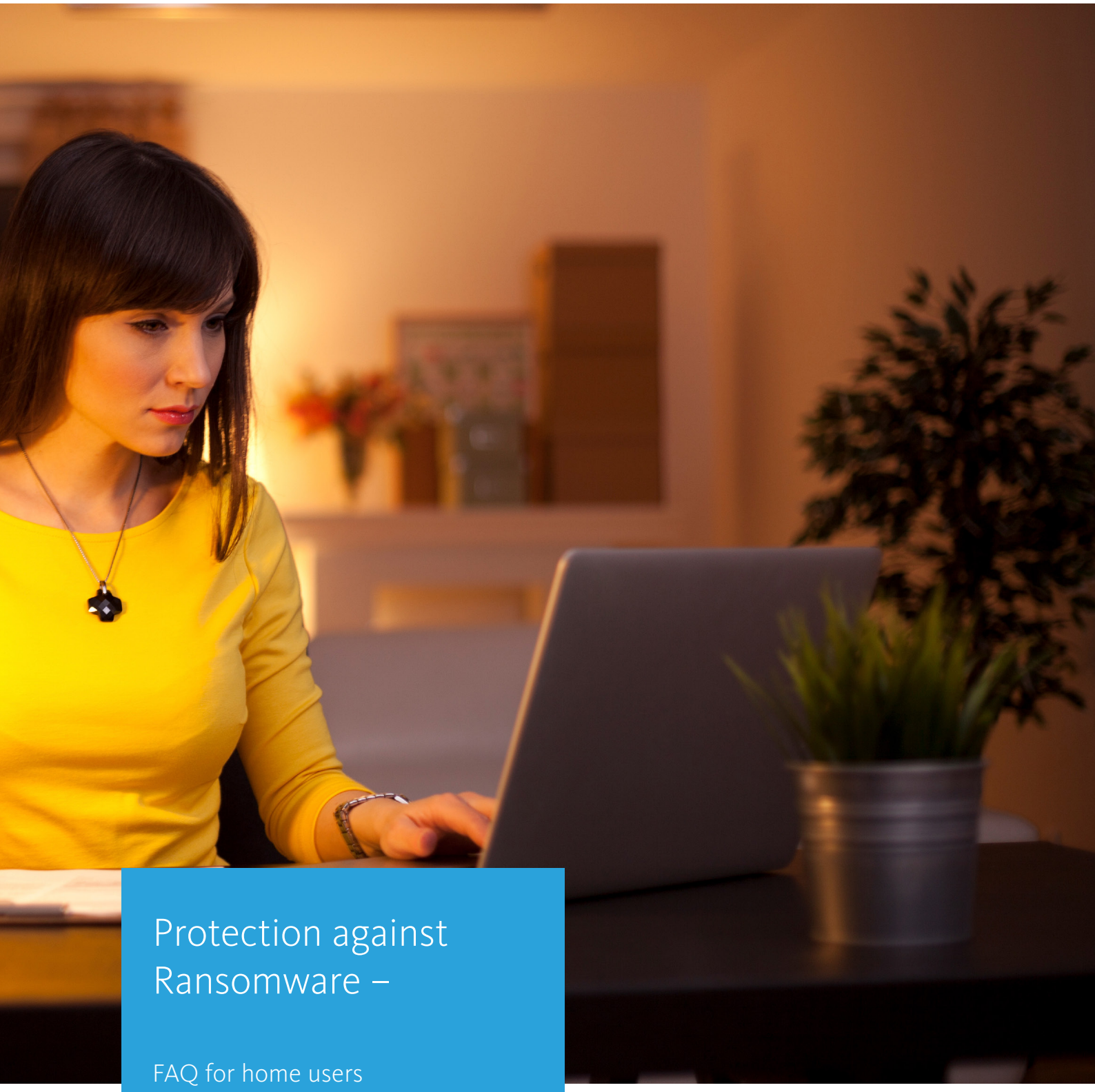
Avira



Protection against Ransomware –

FAQ for home users

www.avira.com

1. What is ransomware?

Ransomware is a type of blackmail malware that encrypts photos, video, music, and other files on a computer or blocks access to the entire system. To access your files or devices again, typically victims need to pay some sort of a ransom or fee.

2. What types of ransomware are there?

Three types of ransomware exist: Encryption ransomware, which scrambles files (making them unusable); lockscreen ransomware, which shows a full-screen image that prevents you from accessing your PC or files; and master-boot-record ransomware, which encrypts the first sector of the partition table on BIOS-based computer systems.

3. What does ransomware do?

Ransomware is typically spread by email or through exploits. In the first instance, the cybercriminal sends a phishing email with an attachment to a specific organization, for example. The unsuspecting user opens this attachment (Word or JavaScript file) as what is written in the email seems deceptively true to the victim. Once the Word document is opened, the user is informed that macros need to be activated to show the content correctly. Enabling macros allows the ransomware to be secretly downloaded onto the computer via a drive-by download by running a script stored in the file.

4. What happens when ransomware infects the computer?

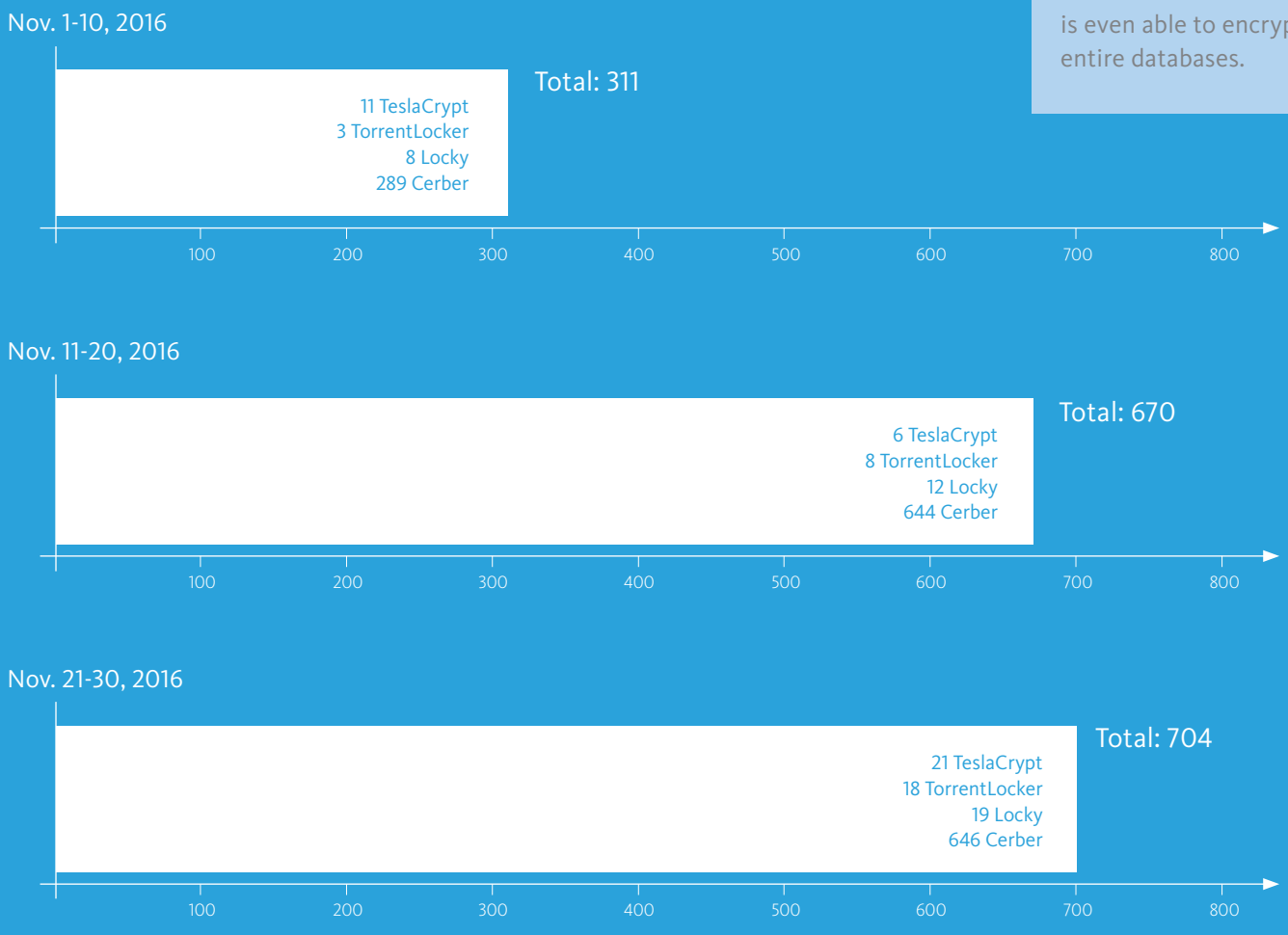
The downloaded crypto-ransomware encrypts all your files, such as photos, videos, and Office documents. It also scrambles data on removable drives and cloud storage services if you are connected to them at the time. Now that all the files have been encrypted using a special file extension, the ransomware demands payment in exchange for unscrambling them. The ransom, which frequently needs to be paid in bitcoins to a special website on the darknet, can amount to many thousands of euros. In the case of screen-locking ransomware, the malware locks the home screen – preventing users from accessing their devices – and similarly demands payment for regaining access such as in the form of purchasing a UKash card or other digital payment method.

5. What is the current threat level?

Ransomware attacks will continue as this business model is like a modern-day gold rush for cybercriminals, with many victims willing to pay – often tacitly. Cybercriminals are continuously developing this lucrative business model. This means that nowadays not only Windows programs (Portable Executable) are used, but script languages – VBS, JavaScript, PowerShell – are increasingly also utilized to make malware classification more difficult. Ransomware is now also on Android devices: Users cannot use their smartphone until they buy back their data via text message payment. Mac users are affected by the KeRanger ransomware, among others. Other well-known types include Petya, FBI Ransomware, and Locky, which have already infected millions of Windows computers.

Ransomware – a persistent threat

Volume of selected encryption Trojans
in November 2016 | Source: ransomwaretracker.abuse.ch



Cerber

The Cerber family is one of the most dangerous types of ransomware, which typically spreads in the form of email attachments. The latest version is even able to encrypt entire databases.

6. Which security technologies does Avira employ to fight ransomware?

A multi-layered security approach is needed to minimize and mitigate ransomware risk factors. To achieve this aim Avira has developed efficient technologies to detect and fight malicious software in real time. We employ state-of-the-art technology such as machine learning/artificial intelligence, reputation, behavior-based detection, and real-time analyses to classify unknown files. And as a user you always have access to the most current data thanks to our cloud service. In the future, systems supported by artificial intelligence will play a major part in analyzing and classifying previously unknown malicious software.

Five tips for maximum protection against ransomware:

1

Install antivirus software on all of your devices

Use a virus-protection solution on all of your devices (PC, Mac, smartphones, and tablets).

Avira detects and blocks all known ransomware threats.

2

Be careful with suspicious-looking emails and links

Only open email attachments sent by people you know. Only click trustworthy links and social media posts.

3

Keep all your programs up to date

Always install software updates and patches immediately. This makes it more difficult for ransomware to infect your computer and devices. Make sure that the software on all your devices is up to date to prevent any vulnerabilities. If you are unsure how to keep your software constantly up to date, thereby preventing weak spots, a tool such as Avira Software Updater can help. It alerts you if you have any outdated software on your system, and saves you the hassle of searching for updates.

4

Backup your data regularly

We recommend backing up your data to the cloud or an external drive regularly. If your files should ever get scrambled by ransomware, this way you can simply format your hard disk – safe in the knowledge that all of your data is backed up externally.

5

Use a form of browser protection – or better still, a secure browser like Avira Scout

Avira's free browser extension blocks malicious websites and protects your privacy.

Avira Scout blocks malicious websites and phishing sites automatically, and includes an anti-tracking function. This makes Avira's browser one of the few available that does not collect any data on which websites you visit, what you download, and what you buy online.

About Avira

Avira, a family-owned company which enjoys above-average growth, was founded in 1986 by the IT security pioneer Tjark Auerbach in Tettnang. It is one of the most important regional employers in the Lake Constance area.

For three decades, Avira has provided its customers with security solutions, developed by Avira itself, for protection against Internet threats, malware attacks, harmful programs, and data theft. More than 100 million users, particularly micro and small businesses as well as home users, rely on Avira's software and value its reliability, performance, and usability.

Avira ranks second among the world's leading antivirus software manufacturers. The company, headed by Travis Witteveen, operates its own virus laboratories and continuously demonstrates its enthusiasm for innovation and its capabilities by developing next-generation security technologies. These include real-time protection through cloud-based malware detection and the "Online Essentials" Web Console.

Avira works closely with the Federal Office for Information Security (BSI) and is a founding member of the "IT-Security made in Germany" initiative.

Avira's experience and top-rated products and services help people move freely and safely in our digital world.

Security in the real world is another important concern for Avira. Established by the company's founder, the Auerbach Foundation supports charitable and social projects, and has already sponsored more than 300 projects in the areas of education and schooling, children, youth and family, assistance for senior citizens and people with disabilities, as well as arts and culture.

Avira

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Germany
Phone: +49 (0) 7542-500 0

Errors excepted. Subject to technical changes. As at: December 2016

PROTECTING PEOPLE
IN THE CONNECTED WORLD

www.avira.com