Safe surfing on public WiFi

Public WiFi is cool, particularly when it's offered provider-independent and free of charge as a community service by Freifunk (http://freifunk.net/worum-geht-es/technik-der-community-netzwerke/). Being able to to connect while out and about, at a café, waiting at the train station or airport or even while shopping in town, without using up your data plan: What's not to like? However, many people are still not aware of the risks entailed in public WiFi and accessing the internet via public hotspots. Once we are aware of the risks, we can understand what's OK and what isn't – and take precautions to make surfing via public WiFi access virtually as safe as at home.

A matter of trust

Depend on it: you can't trust anyone in a public WiFi network, and you have to assume that other users can intercept both incoming and outgoing data. In principle, anyone accessing the same hotspot as you can also intercept all communication passing through it. You don't have to be a network wizard anymore to tap into mobile users in a café while they're updating their Facebook statuses or checking their bank balance. All you need is a smart phone and the right app.

These apps make sophisticated network technology available to everyone: the nice kid with the smart phone at the next table could be running a man-in-the-middle attack using ARP spoofing – even if he has no clue about what Address Resolution Protocol (ARP) does. It's no longer just about eavesdropping: attackers can extract and exploit security-relevant data – enabling them to hijack your Facebook account or your banking app (http://www.heise.de/ct/artikel/Die-Hotspot-Falle-1394646.html).

Scared? Don't let scenarios like this spook you. If you've been communicating openly via the internet, for instance by sending unencrypted emails, you can of course continue to do this via public WiFi. But you need to be aware that someone may be reading your data at all times – admittedly, you may decide this is acceptable and transmit only data that you would write on a postcard. However, as soon as sensitive data is concerned, such as passwords or confidential information, you need to be careful: There are precautions and actions you can implement that will keep you relatively safe even in public WiFi networks.

With regard to email, we've already mentioned the operative word: encryption. When the data transmitted via WiFi is encrypted, listeners are helpless: they see only trash, and

Note on use: Opinion of independent expert, Jürgen Kuri, vice-editor in chief of computer publication c't - magazin für computertechnik / heise online on behalf of the NRW State Chancellory. This text may be duplicated and disseminated under the Creative Commons Attribution-NoDerives license 3.0 Germany (CC BY-ND 3.0 DE). For details see https://creativecommons.org/licenses/by-nd/3.0/de/The following must be specified when used: author, client and license (designation and URL).

cannot decrypt the data even with a strong cryptographic attack. You can realize encryption in public WiFi on different levels – with varying levels of complexity and effort for you as the user.

Ways and means

The simplest method is what's called transport encryption. It's simple, at least for you as the user: You only need be sure and select a secure https connection with a website or online service. When communicating with your bank electronically, you should always make sure you use the https access page anyway; most banks no longer permit any other kind of access for online banking. Modern browsers indicate activation of encrypted transport not only in the URL https://… but also show a padlock symbol in the address bar.

Many email providers also offer transport encryption. If you use a browser-based Web mail service, select https access here as well. If you are using an email client, you need to configure it specifically for encrypted transport: In the setup tab, select email transfer via SSL or TLS and the corresponding authentication method (usually via password). The providers publish the necessary information – however, many support transport encryption only in the fee-based version of their email access.

Many other online services, such as Facebook, also offer secure browser access via https. You should choose this method whenever possible. And not only when connecting via public WiFi. Transport encryption secures your communication when using WiFi to access the internet at home as well. Even when your home WiFi is closed and encrypted, the data is transmitted unencrypted along the further transport stages unless you change this.

App as app can

When you're out and about with your smart phone or tablet, you can of course use such methods for your online services and email too. However, apps, for instance instant messaging or chat apps, are more difficult. Here, you need to depend on the apps themselves to encrypt the data – which they often don't do. In that case, you need to decide whether the confidentiality of the communication is important enough that you prefer not to communicate via public WiFi.

For instance, WhatsApp did not support any kind of encryption for a long time. Currently (December 2015), WhatsApp offers message encryption only in the versions for smart phones running Google's Android system, such as those made by Samsung, HTC or Sony. However, as WhatsApp does not show you which system version the other party is using, encrypted communication via WhatsApp is never really secure.

The case is different for chat and messaging clients with built-in encryption. The best-known example of these is Threema, and the most important open-source apps are

Telegram and TextSecure. iMessage also offers encryption of messages between the parties – however, this is only available on Apple systems. All alternatives to WhatsApp have one major disadvantage: We can reach most of the people we want to “talk” to via WhatsApp, because they’re using it anyway. For alternative message apps, you need to convince your partners to switch and install the respective app.

Use of public WiFi is often problematic for other apps as well. You as a user can rarely determine whether apps with an online payment function, for instance, truly encrypt sensitive data for transmission. Some companies have promised improvements in this area, such as Apple with the Transport Security app promised for iOS version 9. But right now that’s only a promise. Aside from that, you can’t really determine whether the app is truly so bug-free that malicious individuals can’t exploit it. Therefore, you should consider whether it’s really a good idea to use public WiFi for important applications that entail account information and payment systems every single time.

End-to-end

Encryption of the data to be transmitted directly in the applications is often referred to as end-to-end encryption. Its advantage over transport encryption is that only you and the other party can access the data – in transport encryption the online service/email provider can naturally read the messages, as it decrypts the data prior to delivery to the recipient. That’s convenient for you, but not one hundred percent secure.

In end-to-end encryption, on the other hand, that data is encrypted at the sending end and only decrypted by the recipient. Today, this is realized using something called asynchronous encryption: Every user has two keys, a private key and a public key. When someone wants to send you a message, they first encrypt it with your public key. This email can only be decrypted using your private key – which only you should know. These “keys” are actually complex software constructs that are generated for you by systems such as PGP: you keep the private key to yourself and distribute your public key to your friends and acquaintances. You can also use public key servers for this, so that anyone who wants to send you an encrypted email can learn your public key easily.

For Windows systems, Gpg4Win (http://www.gpg4win.de) is the system of choice for PGP email encryption. There are also plug-ins for Outlook and for the extremely popular email client Thunderbird (https://www.enigmail.net/download/). Mac users can use GPG Suite (https://gpgtools.org); under iOS, you can also use iPGMail (https://ipgmail.com/). On Android devices, you can use e.g. OpenKeychain (http://www.openkeychain.org/about) in conjunction with the email program K9. All these tools claim to be simple to set up and use, but they aren’t really. If you are uncertain, ask a more knowledgeable acquaintance to help you set up encryption for your email system.

For Web mail services however, there is not yet a simple way to realize end-to-end encryption. Some providers, such as United Internet with GMX and Web.de, are now offering PGP in their Web mail service. If your email provider does not offer this, you

should think about switching to a conventional email client like Thunderbird or set up a mail app on your smart phone or tablet that can also implement encrypted communication.

Fundamental protection

However, email encryption and other protection implemented directly in the applications cannot protect all information from intruders. For instance, the content of the email itself is protected but not the transport information. It is still possible to see who has been emailing with whom, and this can potentially reveal information on confidential communications that one does not necessarily wish to see become public knowledge.

But end-to-end communication can not only be realized using the applications. Using a kind of encrypted “network within the network”, it is possible to encrypt all data traffic leaving your smart phone, tablet or notebook before it is put on the network so that it can only be decrypted by the recipient. This is known as a Virtual Private Network (VPN). As a user, you can be sure that all your communication and data is encrypted. However, the work entailed in setting this up is much greater, and you need to accept that a VPN (http://www.heise.de/netze/artikel/Hotspot-aber-sicher-221475.html) also consumes a certain amount of processing power on your device.

Using VPN, you can even access your home network safely via public WiFi and internet – provided of course that you have installed a VPN server at home and a VPN client with the corresponding access data on your mobile device. Many offices and enterprises use VPN to enable employees to access the internal network via the internet. If you’re willing to take on the additional setup and configuration work, the result is a secure access to your home network from anywhere in the world – and from there back to the internet, without sharing any information with the nosy neighbor at the next table. OpenVPN (https://openvpn.net/) under Linux is generally considered to be the software of choice for such purposes. However, users with a Fritz!Box-brand router at home can simply use its VPN function.

Service providers have already caught on to the fact that configuring a VPN is not for everyone. You can also obtain VPN as an online service – you can then connect with the VPN server of your service provider via public WiFi using a VPN client on your tablet, smart phone or notebook. This operates as a kind of gateway that lets you encrypt all your communication – and ensures that your data are transmitted to the intended destination. Unlike a VPN you set up yourself, however, you have to trust your service provider to handle your data securely and avoid any carelessness – something that tests conducted by the computer magazine c’t reveal is not always the case.

Healthy skepticism, worry-free use

But however you look at it, every user can reliably secure their communication via public WiFi for many types of applications. Those who just want to pass the time by browsing

and are not worried about people looking over their shoulder can go ahead and do so in a public hotspot without any special precautions.

But you should certainly use encryption for communications that you'd rather keep confidential – how you choose to do so and whether you go as far as a VPN depends on how much security you feel you need. For personalized data whose unauthorized release would hurt you, you should consider whether it would be better to use your 3G/4G link – particularly when such important data as online banking access is concerned, you should only operate outside your personal network access in grave emergencies. Even in your home network, your communication is only as secure as you make it – encryption, consistently updated software and protection against malware are strong defenses at home as well.

By observing these measures, you can enjoy your digital lifestyle on the go safely, simply and conveniently using public WiFi and community wireless.

Further information

- Freifunk: German community wireless
http://freifunk.net/worum-geht-es/technik-der-community-netzwerke/

- Free community wireless in practice - brochure with introduction, background and history of Freifunk by Medienanstalt Berlin-Brandenburg
http://www.mabb.de/files/content/document/Publikationen/Freifunk-Broschuere/freifunk_publikation_webversion.pdf

- Die Hotspot-Falle: Gefahren in öffentlichen Funknetzen
http://www.heise.de/ct/artikel/Die-Hotspot-Falle-1394646.html

- Cool bleiben am Hotspot: Maßnahmen zur sicheren WLAN-Nutzung
http://www.heise.de/artikel-archiv/ct/2012/01/088_Cool-bleiben-am-Hotspot

- Das Bestiarium: Angriffe auf Hotspot-Nutzer
http://www.heise.de/artikel-archiv/ct/2012/01/082_Das-Bestiarium

- Hotspot, aber sicher: Funknetze unterwegs mit VPN benutzen ohne Abhörgefahr
http://www.heise.de/netze/artikel/Hotspot-aber-sicher-221475.html

- Gespräche im Flüsterton: Verschlüsselnde Messenger-Apps im Alltagseinsatz
http://www.heise.de/ct/ausgabe/2015-13-Test-Verschluesselnde-Messenger-Apps-im-Alltagseinsatz-2662824.html

- Mitleser-Sperren: Alternative Dienste für komfortable und abhörsichere Mail-Kommunikation

http://www.heise.de/ct/ausgabe/2015-13-Test-Alternative-Dienste-fuer-komfortable-und-abhoersichere-Mail-Kommunikation-2661636.html

- Virtuelle Privatsphäre: So viel Schutz bieten VPN-Dienste
http://www.heise.de/ct/ausgabe/2013-20-Test-So-viel-Schutz-bieten-VPN-Dienste-2314876.html

- Gpg4Win and GnuPG – PGP for Windows
http://www.gpg4win.de/

- Enigmail – PGP plug-in for Thunderbird
https://www.enigmail.net/download/

- iPGMail – PGP for iOS
https://ipgmail.com/

- GPG Suite – PGP for Mac OS X
https://gpgtools.org/

- OpenKeychain – PGP for Android
http://www.openkeychain.org/about/

- OpenVPN – open-source VPN for everyone
https://openvpn.net/