https://www.avira.com/en/blog/the-dangers-of-working-with-free-wi-fi

# خطرات استفاده از Wi-Fi رایگان

امروزه تمایلات افراد برای گذارندن زمان و حتی صرف یک قهوه در رستوران‌ها و کافی‌شاپ‌ها بخصوص در محیط‌های فضای باز در دوران فراگیری ویروس کرونا رو به افزایش است. شاید قبلا معمول نبود که کافه‌ها و سایر مکان‌های عمومی پر از افرادی باشند که مشغول تایپ کردن روی لپ تاپ‌های خود هستند و تمام وقت خود را در آنجا بگذرانند، اما اکنون بسیاری از افرادی در فضاهای عمومی زمان خود را می‌گذرانند و به دنبال آن برای رفاه بیشتراز وای فای عمومی و رایگان استفاده می کنند که می‌تواند منجربه دردسرهایی شود و آن‌ها را در معرض خطر قرار دهد.

ما در اینجا شما را از وجود این خطرات آگاه می‌کنیم و به شما خواهیم گفت در صورت مواجه با آن چه کاری می‌توانید انجام دهید!؟

## خطرات استفاده از وای فای رایگان نا امن در یک نگاه

1. اطلاعات مربوط به آیدی و رمزهایتان را دریافت کند.
2. به داده‌هایی که توسط گوشی و یا کامپیوترتان در حال رد و بدل شدن است دسترسی داشته باشد.
3. به کامپیوتر شما، شبکه و داده‌هایتان دسترسی پیدا کند.
4. بر روی دستگاهتان یک بدافزار مخرب پیاده کند.
5. حسابی که شما در حال استفاده از آن هستید را بدزدد، وارد همان حساب شده و برای اهدافی شوم مورد استفاده قرار دهد.

## بررسی جامع خطرات استفاده از Wi-Fi رایگان

* تهدیدات آنلاین می‌تواند به اشکال مختلف باشد، اما یکی از جدی ترین خطرات، سرقت اطلاعات شخصی است. اگر یک هکرموفق شود از طریق شبکه Wi-Fi به داده های شما دسترسی پیدا کند، می‌تواند به اطلاعات ورودی سیستم، اطلاعات مالی، تصاویر و سایر اطلاعات شخصی شما دسترسی پیدا کند و پس از آن به روش‌های مختلف از آن سوء استفاده کند که هیچ یک مثبت نخواهد بود.
* بعضی اوقات ممکن است تهدید هکرها، سازمانی که شما در آن مشغول به کار هستید را در معرض خطر قرار دهد. استفاده از سیستم شرکتی از Wi-Fi عمومی، به طور بالقوه شرکت را در معرض حملات و سرقت اطلاعات حساس قرار می‌دهد. اگرچه، بیشتر شرکت ها اکنون از نرم افزار آنتی‌ویروس برای جلوگیری از این اتفاق استفاده می کنند، اما این موضوع همچنان می‌تواند منجر به ردیابی و دزدیده شدن اطلاعات شما یا همکار شما شود.
* حملات انسان در میانه راه نیز تهدیدی بسیار برجسته است، این زمانی اتفاق می‌افتد که هکرها، شبکه‌ای را برای جلب توجه کاربران با اسم وای‌فای رایگان به وجود می آورند. آنها اغلب این کار را در مکان‌هایی انجام می‌دهند که مردم خواهان وای فای رایگان هستند. هکرها پس از اتصال به شبکه خود، می‌توانند شروع به جمع آوری اطلاعات هویتی و اطلاعات مالی کنند. نام این شبکه‌ها اغلب شبیه نام کافه، هتل یا فروشگاهی است که در آن نزدیکی می‌باشد، شما باید همیشه دقت کنید و که نام آن را از نظر غلط املایی بررسی کنید. در صورت عدم اطمینان، همیشه با یکی از کارمندان مربوطه تماس بگیرید تا از صحت شبکه وای فای مطمدن شوید.
* بدافزارخطر دیگری است که ممکن است با آن مواجه شوید. بدافزار را می توان به بسیاری از زیر مجموعه‌ها مانند ویروس‌ها ، باج افزارها و موارد دیگر تقسیم کرد. شخصی در همان شبکه می‌تواند بدون اطلاع شما به راحتی بدافزار را روی دستگاه شما کار بگذارد. این بدافزار حتی پس از قطع اتصال از شبکه نیز به کار خود ادامه می‌دهد.

### برای رهایی از دست هکرها چه کارهایی می‌توان انجام داد؟

همه این تهدیدها ممکن است ترسناک به نظر برسند، ما برای آگاهی بیشتر اطلاعاتی را در اختیار شما قرار می‌دهیم که می‌توانید برای حفظ امنیت خود انجام دهید. در مرحله اول، بدانید که به چه چیزی متصل می‌شوید. اطمینان حاصل کنید که به یک شبکه قانونی ارائه شده توسط مشاغل وصل هستید و شرایط و ضوابط، خصوصاً در مورد استفاده و جمع آوری داده‌های خود را بخوانید.

راه‌ حل دوم این است که به راحتی اطلاعات خود را در اختیار قرار ندهید. این اطلاعات ممکن است اطلاعاتی باشد که شما برای ثبت نام در شبکه از آن استفاده می کنید، لطفا از دادن اطلاعات شخصی یا استفاده از مشخصات بانکی خودداری کنید، آگاه باشید که این اطلاعات به راحتی توسط هکرها جمع آوری و استفاده می شوند.

در آخر، یکی از مفیدترین راه‌های جلوگیری از خطر استفاده از شبکه خصوصی مجازی VPN است. با این کار شما به یک سرور ایمن متصل خواهید شد و داده های دستگاه شما رمزگذاری می شود. این یک روش عالی برای جلوگیری از تهدیدات آنلاین است و استفاده از آن برای شما هزینه زیادی نخواهد داشت.

هنگام استفاده از شبکه‌های باز خطرات زیادی پیش روی ما قرار دارد، اما روش هایی نیز برای به حداقل رساندن این خطرات نیز وجود دارد. به کاربران توصیه می شود که هرگز به وای فای های رایگان بدون پسورد و ناشناخته متصل نشوند و اگر هم متصل شدند، به هیچ عنوان وارد حساب های بانکی خود نشوند. پس هوشیار بمانید و هکرها اجازه ورود به سیستم خود را ندهید.

The dangers of working with free Wi-Fi

With the UK slowly opening back up again there’s a natural desire to get out of the house as much as possible. Whether that be going out for dinner, starting a new hobby, or even just working in a different environment. Pre-pandemic it was not uncommon to see cafes and other public areas filled to the brim with people busy typing away on their laptops and post pandemic this is likely to continue. It’s easy to see why this way of working may appeal to people, after being stuck at home for over a year, working in a cafe or a pub may seem like a luxury too good to pass up. However, many people using these public spaces will also be using public, free Wi-Fi which can lead to a whole world of dangers and leave you exposed. So what are these dangers and what can you do?

What’s the harm with free Wi-Fi?

Threats online can come in many different forms but one of the most serious risks is theft of personal information. If a hacker manages to access your data through a compromised Wi-Fi network, they could have free reign over your login credentials, financial information, pictures, and other personal data. Once obtained, hackers can use this information for a variety of reasons, none of which are positive.

Sometimes the threat from hackers may be business orientated. By using a company device on public Wi-Fi, you are potentially exposing the company to attacks and theft of sensitive information. However, most companies do now use features to prevent this from happening, it could still lead to your or your colleague’s data being tracked and sold to advertisers.

Man in the middle attacks are also a very prominent threat, this is when a hacker sets up a network to lure users in by making it look like a free, open network. They will often do this in places where people are expecting some form of free network. Once connected to their network, the hackers can begin to harvest data and financial information. The names of these network will often resemble that of the cafe, hotel, or pub that is nearby, but it is always important to check the name carefully for any spelling mistakes and if unsure, always check with a member of staff to confirm it is their network.

A further risk is malware. Malware itself can be split up into many sub-categories such as adware, viruses, ransomware, and more. Someone on the same open network could easily plant malware on your device without your knowledge. This malware would continue to act even after you had disconnected from the network.

What can I do about it?

All these threats may seem scary, and rightly so, it’s important to stay aware of what’s out there and there are steps you can take to stay secure. Firstly, know what you are connecting to. Ensure you are connecting to a legitimate network provided by the business and read the terms and conditions, especially surrounding the use and collection of your data.

Another step you can take is simply don’t give away too much information. This may be through signing up or whilst you’re using the network, avoid giving away personal information or using bank details and these may be easily collected and used by hackers.

Finally, one of the most useful ways to prevent risk is by using a virtual private network (VPN). This will connect you to a secure server and encrypt the data going to and from your device. This is a great way to prevent online threats and won’t cost you a fortune to use.