نکاتی برای استفاده ایمن از Wi-Fi عمومی

عوامل مخرب می‌توانند از آنلاین شدن شما سوءاستفاده کنند. برای اطلاع از نکاتی که در زمان نیاز به استفاده از Wi-Fi عمومی باید در نظر داشته باشید، توضیحات زیر را مطالعه کنید.

در پاسخ به شیوع ویروس کرونا و تعطیلی کسب و کارها و کتابخانه‌ها، بسیاری از ما زمان بیشتری را به صورت آنلاین سپری می‌کنیم. در نتیجه، ممکن است لازم باشد برای اتصال به اینترنت از Wi-Fi عمومی استفاده کنیم. اگر احساس کردید در موقعیتی قرار دارید که لازم است از یک Wi-Fi عمومی استفاده کنید، لطفاً برای کمک به حفاظت از داده‌های خود به توصیه‌های زیر از طرف Chief Privacy Officer (مأمور ارشد حریم خصوصی) ایالاتی، توجه کنید:

1. از اتصال به شبکه درست اطمینان پیدا کنید.

مطمئن شوید به شبکه مناسب وصل شدید. عوامل مخرب ممکن است شبکه‌هایی ایجاد کنند که به خاطر نامی که دارند بی‌خطر به نظر می‌رسند، اما در حقیقت شما را به سمت اتصال به شبکه‌ای هدایت می‌کنند که برای مشاهده پیمایش شما در اینترنت طراحی شده است. این یعنی اگر اطلاعات ورود به سیستم یا رمز عبور خود به یک وب‌سایت را وارد کنید، هکر قادر به سرقت اطلاعات شما خواهد بود. برای حفاظت از خود در برابر این اتفاق، نام شبکه را به دقت بخوانید و در صورت امکان از یکی از کارکنان بخواهید برای اطمینان از معتبر بودن شبکه، علامت کسب و کار را بررسی کنند.

شبکه‌های شناخته شده، مثل شبکه قهوه‌فروشی‌های زنجیره‌ای و معروف، معتبرتر هستند، زیرا شرکت این شبکه اینترنت را به عنوان یکی از خدمات مربوط به کسب و کار خود، اداره می‌کند. شبکه‌های شناخته‌شده معمولاً از شبکه‌های Wi-Fi رایگان و تصادفی که ممکن است در مکان‌های عمومی روی تلفن شما ظاهر می‌شوند، امن‌تر هستند.

2. اتصال خودکار را قطع کنید.

بسیاری از دستگاه‌ها (تلفن‌های هوشمند، لپ‌تاپ‌ها و تبلت‌ها) تنظیمات اتصال خودکار دارند. این تنظیمات به دستگاه شما اجازه می‌دهد به راحتی به شبکه‌های نزدیک متصل شود. این کار برای شبکه‌های مورد اعتماد هیچ اشکالی ندارد، اما ممکن است دستگاه شما را به شبکه‌هایی متصل کند که احتمالاً امن نیستند. می‌توانید از قسمت تنظیمات دستگاه خود، این ویژگی را غیرفعال کنید. این ویژگی را، خصوصاً در هنگام سفر به مکان‌های ناآشنا، خاموش نگه دارید. برای احتیاط بیشتر، پس از استفاده از Wi-Fi عمومی می‌توانید گزینه «فراموشی شبکه» را انتخاب کنید.

علاوه بر این، در هنگام حضور در مکان‌های عمومی باید مراقبت Bluetooth خود هم باشید. اتصال Bluetooth به دستگاه‌های مختلف اجازه می‌دهد با یکدیگر تماس بگیرند و یک هکر می‌تواند از یک سیگنال Bluetooth روشن برای دسترسی به دستگاه شما استفاده کند. در هنگام حضور در مکان‌های ناآشنا، این عملکرد را روی تلفن و سایر دستگاه‌های خود خاموش نگه دارید.

3. اشتراک فایل را خاموش کنید.

در زمان استفاده از Wi-Fi عمومی، مطمئن شوید گزینه اشتراک فایل خاموش است. می‌توانید با مراجعه به قسمت ترجیحات سیستم یا پانل کنترل، بسته به سیستم عامل دستگاهتان، گزینه اشتراک فایل را خاموش کنید. AirDrop یکی از نمونه‌های ویژگی اشتراک فایل است که باید خاموش کنید. در بعضی سیستم عامل‌ها مثل Windows/رایانه با انتخاب گزینه «عمومی» در هنگام اتصال به یک شبکه عمومی برای اولین بار، امکان اشتراک فایل را خاموش می‌کند.

مراحل خاموش کردن اشتراک فایل

روی رایانه:

1. به شبکه و سپس مرکز اشتراک‌گذاری بروید.
2. سپس تنظیمات اشتراک پیشرفته را تغییر دهید.
3. اشتراک فایل و چاپگر را خاموش کنید.

برای مک:

1. به ترجیحات سیستم بروید.
2. اشتراک را انتخاب کنید.
3. گزینه همه موارد را غیرفعال کنید.
4. پس از آن در فایندر، روی گزینه AirDrop کلیک و این گزینه را انتخاب کنید، به من اجازه بده کشف شوم توسط: هیچکس.

برای iOS، فقط AirDrop را در مرکز کنترل پیدا و خاموش کنید.

4. از یک VPN استفاده کنید.

به نصب یک VPN (شبکه خصوصی مجازی) روی دستگاه خود فکر کنید. یک VPN امن‌ترین گزینه برای داشتن حریم‌خصوصی دیجیتال روی Wi-Fi عمومی است. این نرم‌افزار داده‌های عبوری و ارسالی دستگاه شما را رمزگذاری کرده و به عنوان یک «تونل» حفاظتی عمل می‌کند، در نتیجه داده‌های شما در زمان عبور از یک شبکه قابل مشاهده نیست.

5. هشدار FBI درباره وب‌سایت رمزگذاری شده – HTTPS.

FBI هشدار داده است بعضی وب‌سایت‌ها با آدرس‌هایی که با «https» شروع می‌شوند، امن نیستند. وجود «https» و دکمه قفل باید نشانگر این باشند که ترافیک اینترنتی رمزگذاری می‌شود و بازدیدکنندگان می‌توانند به شکلی ایمن داده‌ها را به اشتراک بگذارند. با این وجود، اکنون متخلفان اینترنتی روی اعتماد عموم حساب کرده و مردم را به سمت وب‌سایت‌های متخلفی که از https استفاده می‌کنند و به ظاهر امن به نظر می‌رسند، اما امن نیستند، هدایت می‌کنند.

توصیه‌های FBI:

- صرفاً به نام روی ایمیل اعتماد نکنید: هدف محتوای ایمیل را زیر سؤال ببرید.
- اگر یک ایمیل مشکوک و حاوی یک لینک از یک مخاطب ناشناس دریافت کردید، از طریق تماس یا ایمیل زدن به آن فرد از درست بودن پیام اطمینان پیدا کنید. به یک ایمیل مشکوک به صورت مستقیم پاسخ ندهید.

- وجود غلط املایی یا کلمات اشتباه در داخل دامنه لینک را به دقت بررسی کنید (مثال، اگر یک آدرس که باید با ".gov" تمام شود در انتها ".com" دارد).
- به یک وبسایت صرفاً به خاطر داشتن علامت قفل یا عبارت «https» در نوار آدرس مرورگر، اعتماد نکنید.

6. توصیه می‌شود به اطلاعات حساس دسترسی پیدا نکنید.

حتی اگر یک VPN دارید، باز هم توصیه نمی‌شود روی یک شبکه عمومی و غیرامن به حساب بانک شخصی خود یا داده‌های شخصی و حساس دیگر مثل شماره تأمین اجتماعی دسترسی پیدا کنید. حتی شبکه‌های عمومی و امن هم می‌توانند خطرناک باشند. اگر مجبور هستید از یک Wi-Fi عمومی به این حساب‌ها دسترسی پیدا کنید، تمام دقت خود را به خرج دهید. برای تراکنش‌های مالی، ممکن است بهتر باشد به جای آن از عملکرد هات‌اسپات تلفن هوشمند خود استفاده کنید.

7. امن در مقابل غیرامن.

به طور کلی دو نوع شبکه Wi-Fi عمومی وجود دارد. امن و غیرامن.

هر زمان که امکان داشتید به شبکه‌های عمومی امن متصل شوید. به یک شبکه غیرامن می‌توان بدون نیاز به هیچ ویژگی امنیتی مثل رمز عبور یا ورود به سیستم، متصل شد. برای اتصال به یک شبکه امن معمولاً لازم است کاربر قبل از اتصال به شبکه، با شرایط و ضوابط موافقت کند، یک حساب ثبت نماید یا یک رمز عبور را تایپ کند.

8. دیوار آتش خود را فعال نگه دارید.

اگر از یک لپ‌تاپ استفاده می‌کنید، در زمان استفاده از یک Wi-Fi عمومی، دیوار آتش خود را فعال نگه دارید. دیوار آتش به عنوان یک مانع عمل کرده و از دستگاه شما در برابر تهدیدات مربوط به بدافزارها حفاظت می‌کند. کاربران می‌توانند برای جلوگیری از مشاهده پیام‌های اعلان دیوار آتش Windows خود را غیرفعال کرده و سپس فراموش کنند. اگر می‌خواهید آن را در یک رایانه دوباره راه‌اندازی کنید، به پانل کنترل، «سیستم و امنیت» بروید و سپس «دیوار آتش Windows» را انتخاب نمایید. اگر از Mac استفاده می‌کنید، به قسمت «ترجیحات سیستم»، سپس «امنیت و حریم خصوصی»، بعد زبانه «دیوار آتش» بروید و این ویژگی را فعال کنید.

9. از نرم‌افزار ضدویروس استفاده کنید.

همچنین مطمئن شوید آخرین نسخه از یک برنامه ضدویروس روی لپ‌تاپ شما نصب شده است. برنامه‌های ضدویروس می‌توانند در زمان استفاده از Wi-Fi عمومی با شناسایی بدافزارهایی که احتمال دارد در هنگام استفاده از شبکه مشترک وارد سیستم شما شوند، به شما کمک کنند. اگر ویروس‌های شناخته‌شده روی دستگاه شما بارگیری شوند یا در صورت وجود فعالیت مشکوک و حمله یا وارد شدن یک بدافزار به سیستم، به شما هشدار داده خواهد شد.

10. از تأیید اعتبار دو عاملی یا چند عاملی استفاده کنید.

در زمان ورود به وبسایت‌ها با اطلاعات شخصی، از تأیید اعتبار چند عاملی (MFA) استفاده کنید. این یعنی به یک پیام تأیید دوم (که برای تلفن شما پیامک می‌شود یا از طریق یک برنامه یا کلید فیزیک در اختیار شما قرار می‌گیرد) نیاز دارید تا بیشتر از شما محافظت شود.
بنابراین اگر یک هکر نام کاربری و رمز عبور شما را دریافت کرد، نمی‌تواند بدون داشتن کد تأیید اعتبار به حساب شما دسترسی پیدا کند.

11. مراقب دستگاه‌های شخصی خود باشید.

لپ‌تاپ، تبلت یا تلفن هوشمند خود را بدون مراقبت در یک مکان یا وسیله حمل و نقل عمومی رها نکنید. حتی اگر در زمان اتصال به یک شبکه Wi-Fi احتیاطهای لازم را به کار بگیرید، احتمال اینکه یک نفر وسایل شما را بردارد یا بدون اطلاع شما به اطلاعاتتان نگاهی بیاندازد، از بین نخواهد رفت. مراقب اطراف خود باشید و به کسانی که در کنار شما هستند توجه کنید.

12. سایر نکات برای ایمنی آنلاین.

در این قسمت چند نکته برای حفظ ایمنی آنلاین، به خصوص در زمان استفاده از اتصال به Wi-Fi عمومی، ذکر شده است:

- از رمز عبورهای قوی استفاده کنید.
- دستگاه‌های خود را رمزگذاری کنید.
- مراقبت ایمیل‌های فیشینگ باشید.
- مراقبت آنچه در رسانه‌های اجتماعی پست می‌کنید باشید. اطلاعات فردی بسیار دقیق می‌توانند به هکرها در حدس زدن رمز عبورتان کمک کنند.
- اطلاعات قدیمی را که دیگر نیاز ندارید حذف کنید.
- اگر یک شبکه از شما خواست یک برنامه یا ضمیمه مرورگر اضافه نصب کنید، به آن متصل شوید.
- از نصب جدیدترین بسته‌ها و به‌روزرسانی‌های نرم‌افزاری روی دستگاه‌های خود برای حفاظت در برابر مسائل شناخته‌شده، اطمینان پیدا کنید.