Tipps zur sicheren Nutzung von öffentlichem WLAN

Böswillige Akteure können Sie online ausnutzen. Im Folgenden finden Sie einige Tipps, die Sie beachten sollten, wenn Sie öffentliches WLAN verwenden müssen.

Durch den Ausbruch des Coronavirus und die Schließung von Unternehmen und Bibliotheken verbringen viele von uns mehr Zeit online. Infolgedessen müssen wir möglicherweise öffentliches WLAN für den Internetzugang nutzen. Beachten Sie bitte die folgenden Empfehlungen des staatlichen Datenschutzbeauftragten zum Schutz Ihrer Daten, falls Sie öffentliches WLAN nutzen müssen:

1. Bestätigen Sie, dass Sie das richtige Netzwerk haben.

Stellen Sie sicher, dass Sie sich mit dem richtigen Netzwerk verbinden. Böswillige Akteure können Netzwerke schaffen, die aufgrund ihres Namens harmlos aussehen, Sie jedoch in Wirklichkeit veranlassen, sich mit einem Netzwerk zu verbinden, das Ihre Aktivitäten im Internet verfolgt. Dies bedeutet, dass der Hacker Ihre Daten stehlen kann, wenn Sie Anmeldedaten oder Passwörter in Websites eingeben. Überprüfen Sie den Netzwerknamen daher sehr sorgfältig und fragen Sie, falls möglich, einen Mitarbeiter oder überprüfen Sie die Beschilderung des Unternehmens, um sicherzustellen, dass das Netzwerk legitim ist.

Bekannte Netzwerke, wie die bekannter Kaffeeketten, sind wahrscheinlich weniger verdächtig, weil das Unternehmen das Netzwerk als eine Dienstleistung im Rahmen seiner Geschäftstätigkeit betreibt. Bekannte Netzwerke sind im Allgemeinen sicherer als zufällige freie WLAN-Netzwerke, die auf Ihrem Telefon an einem öffentlichen Ort angezeigt werden können.

2. Schalten Sie Auto-Connect aus.

Viele Geräte (Smartphones, Laptops und Tablets) verfügen über automatische Verbindungseinstellungen. Mit dieser Einstellung können Ihre Geräte bequem mit Netzwerken in der Nähe verbunden werden. Dies ist bei vertrauenswürdigen Netzwerken völlig in Ordnung. Sie kann Ihre Geräte jedoch auch mit Netzwerken verbinden, die möglicherweise nicht sicher sind. Sie können diese Funktion über die Einstellungsfunktion auf Ihrem Gerät deaktivieren.

Lassen Sie diese Einstellungen insbesondere dann ausgeschaltet, wenn Sie an unbekannte Orte reisen. Als zusätzliche Vorsichtsmaßnahme können Sie nach der Verwendung von öffentlichem WLAN „Netzwerk vergessen“ markieren.

Sie sollten außerdem Ihr Bluetooth an öffentlichen Orten überwachen. Die Bluetooth-Verbindung ermöglicht es verschiedenen Geräten, miteinander zu kommunizieren. Ein Hacker kann nach offenen Bluetooth-Signalen suchen, um Zugang zu Ihren Geräten zu erhalten. Lassen Sie diese Funktion auf Ihrem Telefon und anderen Geräten ausgeschaltet, wenn Sie sich in einer unbekannten Gegend aufhalten.

3. Schalten Sie die Dateifreigabe aus.

Stellen Sie sicher, dass die Dateifreigabe-Option ausgeschaltet ist, während Sie sich im öffentlichen WLAN befinden. Sie können die Dateifreigabe je nach Betriebssystem in den Systemeinstellungen oder in der Systemsteuerung ausschalten. AirDrop ist ein Beispiel für eine Dateifreigabefunktion, die Sie ausschalten sollten. Einige Betriebssysteme wie Windows/PC schalten die Dateifreigabe für Sie aus, indem sie die Option „öffentlich“ wählen, wenn Sie sich zum ersten Mal mit einem neuen öffentlichen Netzwerk verbinden.

Schritte zum Ausschalten der Dateifreigabe

Auf einem PC:

1. Gehen Sie zum Netzwerk- und Sharing-Center.
2. Ändern Sie dann Erweiterte Einstellungen.
3. Schalten Sie die Datei- und Druckerfreigabe aus.

Für Mac:

1. Gehen Sie zu Systempräferenzen.
2. Wählen Sie Gemeinsame Nutzung.
3. Wählen Sie alles ab.
4. Klicken Sie im Finder als Nächstes auf AirDrop und wählen Sie Erlaube mir, entdeckt zu werden von: Niemand.

Suchen Sie für iOS einfach AirDrop im Control Center und schalten Sie es aus.

4. Verwenden Sie ein VPN.

Erwägen Sie die Installation eines VPN (Virtual Private Network) auf Ihrem Gerät. Ein VPN ist die sicherste Option für den digitalen Datenschutz im öffentlichen WLAN. Es verschlüsselt Ihre

Daten auf dem Weg zu und von Ihrem Gerät und dient als schützender „Tunnel“, damit Ihre Daten auf dem Weg durch ein Netzwerk nicht sichtbar sind.

5. Warnung des FBI vor verschlüsselten Websites - HTTPS.

Das FBI warnt vor Websites, deren Adressen mit „https“ beginnen. Das Vorhandensein von „https“ und des Schloss-Symbols soll anzeigen, dass der Webverkehr verschlüsselt ist und Besucher Daten sicher austauschen können. Cyberkriminelle setzen nun jedoch auf das Vertrauen der Öffentlichkeit, indem sie Menschen auf bösartige Websites locken, die https enthalten und sicher scheinen, obwohl sie es nicht sind.

Empfehlungen des FBI:

- Vertrauen Sie nicht einfach dem Namen in einer E-Mail: Hinterfragen Sie die Absicht des E-Mail-Inhalts.
- Falls Sie eine verdächtige E-Mail mit einem Link eines bekannten Kontakt erhalten, bestätigen Sie, dass die Nachricht legitim ist, indem Sie den Kontakt anrufen oder ihm eine E-Mail schicken. Antworten Sie nicht direkt auf eine verdächtige E-Mail.
- Prüfen Sie auf Rechtschreibfehler oder falsche Domains innerhalb eines Links (z. B. ob eine Adresse, die auf „.gov“ enden sollte, stattdessen auf „.com“ endet).
- Vertrauen Sie einer Website nicht, nur weil sie ein Schloss-Symbol oder „https“ in der Browser-Adressleiste enthält.

6. Der Zugriff auf vertrauliche Daten wird nicht empfohlen.

Selbst wenn Sie ein VPN haben, ist es immer noch nicht empfehlenswert, auf persönliche Bankkonten oder ähnliche vertrauliche, personenbezogene Daten wie Sozialversicherungsnummern in ungesicherten öffentlichen Netzwerken zuzugreifen. Selbst öffentlich gesicherte Netzwerke können riskant sein. Entscheiden Sie nach bestem Wissen und Gewissen, ob Sie auf diese Konten über öffentliches WLAN zugreifen müssen. Für finanzielle Transaktionen kann es besser sein, stattdessen die Hotspot-Funktion Ihres Smartphones zu verwenden.

7. Gesichert und ungesichert im Vergleich.

Grundsätzlich gibt es zwei Arten von öffentlichen WLAN-Netzwerken: gesicherte und ungesicherte.

Stellen Sie wann immer möglich eine Verbindung zu gesicherten öffentlichen Netzwerken her. Die Verbindung zu einem ungesicherten Netzwerk kann ohne jede Art von

Sicherheitsmerkmalen wie Passwort oder Login hergestellt werden. Ein gesichertes Netzwerk erfordert in der Regel, dass der Nutzer den Geschäftsbedingungen zustimmt, ein Konto einrichtet oder ein Passwort eingibt, bevor er sich mit dem Netzwerk verbindet.

8. Lassen Sie Ihre Firewall aktiviert.

Lassen Sie Ihre Firewall aktiviert, wenn Sie einen Laptop verwenden, während Sie sich im öffentlichen WLAN befinden. Eine Firewall dient als Barriere, die Ihr Gerät vor Malware-Bedrohungen schützt. Nutzer können die Windows-Firewall aufgrund von Pop-Ups und Benachrichtigungen deaktivieren und sie dann vergessen. Gehen Sie zur Systemsteuerung, „System und Sicherheit“ und wählen Sie „Windows-Firewall“, falls Sie sie auf einem PC neu starten wollen. Gehen Sie zum Aktivieren der Funktion zu „Systemeinstellungen“, dann zu „Sicherheit und Datenschutz“ und dann zur Registerkarte „Firewall“, falls Sie Mac-Nutzer sind.

9. Verwenden Sie Virenschutz-Software.

Stellen Sie auch sicher, dass Sie die neueste Version eines Virenschutzprogramms auf Ihrem Laptop installieren. Virenschutzprogramme können Sie bei der Nutzung von öffentlichem WLAN schützen, indem sie Malware erkennen, die bei der Nutzung des gemeinsam genutzten Netzwerks in Ihr System gelangen könnte. Eine Warnmeldung warnt Sie, falls bekannte Viren auf Ihr Gerät geladen werden oder eine verdächtige Aktivität oder ein verdächtiger Angriff erfolgt oder Malware in Ihr System gelangt.

10. Verwenden Sie die Zwei- oder Multi-Faktor-Authentifizierung.

Verwenden Sie die Multi-Faktor-Authentifizierung (MFA), wenn Sie sich mit Ihren persönlichen Daten bei Websites anmelden. Dies bedeutet, dass Sie über einen zweiten Verifizierungscode verfügen (per SMS an Ihr Telefon oder über eine Anwendung oder einen physischen Schlüssel), der Sie zusätzlich schützt. Selbst wenn also ein Hacker Ihren Nutzernamen und Ihr Passwort erhält, kann er ohne einen Authentifizierungscode nicht auf Ihre Konten zugreifen.

11. Lassen Sie Ihre persönlichen Geräte nicht aus den Augen.

Lassen Sie Ihren Laptop, Ihr Tablet oder Smartphone nicht unbeaufsichtigt an einem öffentlichen Ort oder in einem öffentlichen Fahrzeug liegen. Selbst wenn Sie Vorsichtsmaßnahmen in einem WLAN-Netzwerk treffen, wird das niemanden davon abhalten,

Ihr Eigentum zu stehlen oder heimlich einen Blick auf Ihre Daten zu werfen. Seien Sie sich Ihrer Umgebung bewusst und achten Sie auf die Personen um Sie herum.

12. Weitere Online-Sicherheitstipps.

Hier sind ein paar Tipps, wie Sie online sicher bleiben können, insbesondere wenn Sie eine öffentliche WLAN Verbindung nutzen:

- Verwenden Sie sichere Passwörter.
- Verschlüsseln Sie Ihre Geräte.
- Vorsicht vor Phishing-E-Mails.
- Seien Sie vorsichtig, was Sie in sozialen Medien veröffentlichen. Zu viele persönliche Informationen können Hackern beim Erraten von Passwörtern helfen.
- Löschen Sie alte Informationen, die Sie nicht mehr benötigen.
- Stellen Sie keine Verbindung her, wenn ein Netzwerk Sie auffordert, zusätzliche Software oder Browser-Erweiterungen zu installieren.
- Stellen Sie sicher, dass die neuesten Patches und Software-Updates zum Schutz vor bekannten Problemen auf Ihren Geräten installiert sind.