الاتصال الآمن على الشبكات اللاسلكية العشوائية

أصبح للشبكات اللاسلكية دوراً هاماً و فاعلاً في تغيير طريقة استخدامنا للحاسوب و الانترنت، فلكي تتصل بالانترنت لا يلزمك سوى جهاز حاسوب محمول أو حتى حاسوب مكتبي مجهزة ببطاقة اتصال لاسلكية و نقطة الاتصال اللاسلكي (Wireless Access Point). لأن نقاط الاتصال اللاسلكي أصبحت في تزايد مستمر حتى أن العديد من الشبكات المنزلية أصبحت تعتمد عليها بشكل مضطرد. يُمكن للفرد العادي ملاحظة عدد الشبكات اللاسلكية المتوفره في الجوار من خلال معالج الاتصال اللاسلكي و الذي بدوره يعرض كافة الشبكات اللاسلكية ضمن البيئة المُحيطة. و سواءً كان مصدر هذه الشبكات مؤسسات خاصة أو أفراد، فأنها جميعها عرضةً للاختراقات الأمنية، لهذا فإن جزء كبير من مسئولية حماية البيانات يقع على عاتق الأفراد أنفسهم، فيما يلي مجموعة من النصائح لتأمين العمل على الشبكات اللاسلكية في الأماكن العامة:

- **لا تقم بالاتصال على أي شبكة لاسلكية غير آمنة** – فإذا لم تكن انت بحاجة إلى كلمة مرور لكي تتصل بالشبكة اللاسلكية فكذلك الحال مع المخترقين. عند بدء البحث عن الشبكات اللاسلكية المتوفرة، فإن القائمة التي تظهر عادةً ما تُظهر رموزاً خاصة للاعلام عن وجود إعدادات أمان أم لا، و في هذه الحالة ينبغي تجنب الاتصال على أي شبكة لا توفر إعدادات أمان خاصةً تلك التي لا يوجد معلومات عن مصدرها و الجهة التي تقوم بتوفيرها.

- **لا تفترض أن الشبكات اللاسلكية العامة آمنة** – و بدلاً عن ذلك افترض أن كافة الأشخاص الموجودين في جوارك و يتصلون على الشبكة اللاسلكية، قادرين على

معرفة البيانات التي تقوم بإرسالها و استقبالها عبر الاتصال اللاسلكي، و لهذا تجنب التعامل مع البيانات الحساسة مثل كلمات المرور و بطاقات الائتمان أو الحسابات البنكية و ذلك أثناء الاتصال في الشبكات اللاسلكية العامة.

- **تأكد من بيانات الشبكة اللاسلكية قبل الاتصال بها** – فمن السهل لأي مخترق أن يحاكي اسم الشبكة اللاسلكية الآمنة ليتم خداع المستخدمين، فمثلاً يمكن لشخص ما أن ينشئ شبكة لاسلكية باسم IUG W/I في حين أن اسم الشبكة الجامعية هو IUG W/L أو يمكن اختيار أي مُسميات أخرى قريبة و يمكن من خلالها خداع المستخدمين و دفعهم للاتصال على الشبكة الغير معروفة المصدر ، و لهذا فإن التدقيق في اسم الشبكة قبل الاتصال عامل مهم لزيادة الأمان.

- **قم بتعطيل الاتصال اللاسلكي الآلي** – و بدلاً عن ذلك قم بتجهيز حاسوبك لإعلامك عن الشبكات اللاسلكية المُتوفرة قبل الاتصال الفعلي عليها حتى لا تقع فريسة الاتصال على شبكة عشوائية غير آمنة.

- **قم باستخدام جدار حماية ناري** – فمن الضروري استخدام جدار الحماية لحمايتك من وصول الآخرين لموارد حاسوبك، و إذا كان نظام التشغيل لديك يحتوي على جدار حماية داخلي فتأكد من تفعيله.

- **قم بتعطيل مشاركة الملفات و الطابعات** – فهذه الميزات تتيح لك السماح للآخرين بالاتصال على حاسوبك و قراءة الملفات التي تقوم أنت بتحديدها للمشاركة، كما يمكن السماح ايضاً باستخدام الطابعة الموجودة لديك، و غالباً لن تحتاج هذه

الميزات عن الاتصال على شبكة لاسلكية عشوائية، فمن المستحسن عندئذٍ تعطيل هذه الخدمات بشكل كامل حتى لا تزيد فرص الوصول لحاسوبك من قبل الآخرين.

- **إزالة الملفات الحساسة عن الحاسوب المحمول** – فمن المفيد جداً إزالة هذه الملفات الخاصة و التي لن يتم التعامل معها في في خارج مكان العمل، و بالتالي انهاء التهديدات بكشف هذه الملفات بشكل كامل.

دائرة أمن المعلومات