الجمهورية العربية السورية
وزارة الاتصالات والتقانة
الهيئة الوطنية لخدمات الشبكة

National Agency for Network Services

نصائح أمنية لتبقى بأمان عند قيامك بعملك من المنزل

إعداد:
م. نوره قادري

مركز أمن المعلومات

وسط جائحة فيروس كورونا تنتقل العديد من الحكومات من ضمن استراتيجيتها لمكافحة الفيروس إلى تقنيات التباعد الاجتماعي بما في ذلك إغلاق المدارس، ومطالبة الأشخاص بالعمل من المنزل للمساعدة في كسر سلسلة انتشار الفيروس.

إنّ عصر الإنترنت والتقدم التكنولوجي جعل من السهل للغاية بالنسبة للعديد منا القيام بواجباتنا المنتظمة من الأريكة المريحة، حيث يعمل العديد من الأشخاص بدوام كامل من منازلهم، ومع ذلك، فإنّ هذا الترف يأتي مع سلبياته بشكلٍ رئيسي عن طريق التهديدات الأمنية عبر الإنترنت، حيث لا يمكن للعاملين عن بُعد فقط أن تتعرّض خصوصيتهم للخطر، بل قد يؤدّي العمل من المنزل إلى انتهاك أمن الشركات والمؤسسات أيضًا.

في هذه المقالة سنستعرض بعض النصائح لمساعدتك في البقاء آمنًا عبر الإنترنت وحماية أجهزتك ومعلوماتك الشخصية حتى تتمكّن من القيام بعملك براحة واطمئنان.

نبدأ بعرض بعض التهديدات عبر الإنترنت التي يجب أن يكون العاملون عن بُعد على معرفة بها:

- **شبكات الاتصال اللاسلكي غير آمنة:**

قد يضطرّ بعض العمال إلى استخدام شبكات wi-fi العامة غير الآمنة والتي تُعدّ نقاطًا رئيسية للأطراف الخبيثة للتجسس على حركة المرور على الإنترنت وجمع المعلومات السرية.

- **استخدام الأجهزة والشبكات الشخصية:**

العديد من العمال سيضطرون إلى استخدام الأجهزة الشخصية والشبكات المنزلية لمهام العمل. غالبًا ما تفتقر هذه الأدوات إلى أدوات الحماية الموجودة في شبكات الأعمال مثل برامج مكافحة الفيروسات القوية وجدران الحماية وأدوات النسخ الاحتياطي التلقائي عبر الإنترنت، وهذا يزيد من خطر اكتشاف البرامج الضارة طريقها إلى الأجهزة وكذلك تسرّب المعلومات الشخصية والمعلومات المتعلقة بالعمل.

- **عمليات الاحتيال التي تستهدف العاملين عن بُعد:**

من المحتمل أن نشهد زيادة في الهجمات الإلكترونية التي تستهدف العاملين عن بُعد.

مثل عمليات الاحتيال وهجمات التصيد الإلكتروني، لكن إذا كنّا مسلحين بالمعرفة والأدوات الصحيحة، يمكننا درء العديد من هذه التهديدات ومواصلة إنجاز عملنا.

التوصيات والحماية:

قبل أن تتخذ تدابيرك الخاصّة لحماية أمنك على شبكة الإنترنت، يجب عليك التحقق من صاحب العمل الخاص بك لمعرفة ما إذا كان لديهم أي بروتوكولات (في ضوء أزمة COVID-19) قد تكون قادرة على تزويدك بتوجيهات محددة حول كيفية التعامل مع جوانب معينة من الأمن السيبراني وربما توفّر الوصول إلى بعض الأدوات التي تحتاجها.

لحسن الحظ، حتى إذا لم يقدّم صاحب العمل مثل هذه البروتوكولات، أو إذا كنت تعمل لحسابك الخاص، فهناك بعض الخطوات البسيطة التي يمكنك اتّخاذها لحماية نفسك أثناء العمل من المنزل:

1. استخدم كلمات مرور قوية.
2. قم بإعداد واستخدام المصادقة الثنائية two-factor authentication .
3. استخدام شبكات VPN .
4. تفعيل جدار الحماية الخاص بنظام التشغيل على الأقل.
5. استخدام برنامج مكافحة الفيروسات Antivirus software .
6. تأمين جهاز التوجيه المنزلي Router الخاص بك.
7. تثبيت التحديثات الخاصة بنظام التشغيل بانتظام.
8. انسخ بياناتك احتياطيًا.
9. تجنب استخدام أدوات سطح المكتب البعيد.
10. الحذر من رسائل ومواقع التصيد الاحتيالي.
11. احترس من الحيل التي تستخدم فرص العمل من المنزل.
12. استخدم اتصالات مشفرة.
13. اقفل جهازك عند تركه ولو لفترة قصيرة.

دعونا نلقي نظرة على كلٍّ من هذه النصائح ببعض التفصيل:

✓ **استخدام كلمات مرور قويّة**

لسوء الحظ مازال الكثير من الأشخاص يستخدمون نفس كلمة المرور لعدد من حساباتهم الشخصيّة وبهذا يحتاج المهاجم لكلمة مرور واحدة لاختراق جميع الحسابات، حيث يعمل المهاجمون على استخدام أسماء مستخدمين وكلمات مرور مسرّبة ويحاولون تسجيل الدخول إلى حسابات أخرى عبر الإنترنت.

لذا يجب التأكّد من أنّ جميع حساباتك محميّة بكلمات مرور يصعب اختراقها، ويتحقق ذلك بأن تشتمل كلمة المرور على سلسلة طويلة من الأحرف الكبيرة والصغيرة والأرقام والمحارف الخاصة وأن تكون كلمات المرور فريدة لكلّ حساب.

✓ تفعيل المصادقة الثنائية

أن يكون لديك كلمة مرور قويّة أمر غير كاف لتأمين حسابك لذا فإنّ إعداد المصادقة الثنائية Two-Factor Authentication (2FA) والتحقق بخطوتين two-step verification (2SV)، للحسابات الشخصية على الويب هو بمثابة طبقة أمان إضافية لحماية حساباتك الشخصية وذلك عند محاولة الوصول إلى حسابك من أي جهاز آخر.

ويتمثل ذلك بإحدى طرق تأكيد الحساب التالية:

- إدخال رمز تسجيل دخول خاص (قد يصلك كرسالة بريد إلكتروني أو رسالة نصية SMS إلى رقم الجوال الخاص بالحساب)
- استخدام إحدى طرق القياس الحيوية مثل التعرف على الوجه أو بصمات الأصابع إن أمكن.
- استخدام حامل إلكتروني Token الذي تقوم بتوصيله بجهازك.

✓ استخدام الشبكات الافتراضية VPN

كثير من الناس على دراية باستخدام الشبكة الافتراضية الخاصة (Virtual Private Network VPN)، حيث تستطيع الوصول جميع الخدمات والمواقع المحظورة في بلدك نظرًا لأنّ VPN تقوم بتمرير حركة المرور الخاصة بك من خلال مخدّم في الموقع الذي تختاره، فهي مثالية لتغيير الموقع على الشبكة العنكبوتية.

لكن للشبكة الافتراضية الخاصّة دورٌ مهمٌّ آخر، حيث يمكن لكل شركة إنشاء شبكة افتراضية تستخدم التشفير مخصصة للعمل عن بعد، ويمكن من خلالها حصر الوصول لموارد الشركة وخدماتها بالعاملين لديها عن بعد وفق سياسة أمنية مناسبة وصارمة.

مع عمل معظم الموظفين من المنزل في ظلّ انتشار فيروس كورونا(COVID-19) اليوم، أصبحت تمثل خدمة VPN الطريقة الأكثر أمانًا للوصول إلى شبكات الشركة والموارد الخاصة وتُعتبر بمثابة العمود الفقري للشركة، ويجب أن يكون أمنها وتوافرها هو التركيز في المستقبل لفرق تكنولوجيا المعلومات.

ومع قيام العديد من المؤسسات بنقل القوى العاملة لديها إلى وظائف من المنزل، يمكن للمتسللين شنّ هجمات منع الخدمة الموزّعة DDoS (distributed denial-of-service) على مخدّمات VPN واستنفاد مواردهم،

مما يؤدّي إلى تعطل مخدّم VPN والحدّ من توافريته، ولأن مخدّمات الـ VPN تعمل كبوابة لشبكة داخلية للشركة، فإنّ هذا سيمنع جميع الموظفين البعيدين من أداء وظائفهم، مما يؤدّي إلى عملية شلل لخدمات الشركة.

لا يقتصر هذا الهجوم على مخدّمات الويب بل أيضاً شبكات VPN القائمة على SSL (مثل Puls Secure و Fortinet وغيرها) هي عرضةً لهجوم SSL Flood (DDoS) ، حيث يمكن للمهاجمين بدء الآلاف من اتصالات SSL بشبكة VPN SSL، ثم تركها معلّقة وبهذا يتمّ استنفاذ الذاكرة في المخدّم، ومنع لمستخدمين الشرعيين من الوصول للخدمة.

علاوةً على ذلك، من المرجح أن يعمل موظفو تكنولوجيا المعلومات من المنزل، لذلك فإنّ المهاجمين سيستغلّون أي ضعف متبقٍ في مخدّمات VPN لقطع اتصال مسؤولي النظام عن مخدّماتهم الخاصّة أثناء قيامهم بالهجوم من خلال الشبكة الداخلية بهدف سرقة البيانات الخاصة أو تثبيت برامج الفدية RanSomWare لكنّ مخدّمات VPN ستبقى الخيار الأفضل من ضمن مجموعة من أدوات العمل عن بعد والمتاحة في الشركات اليوم.

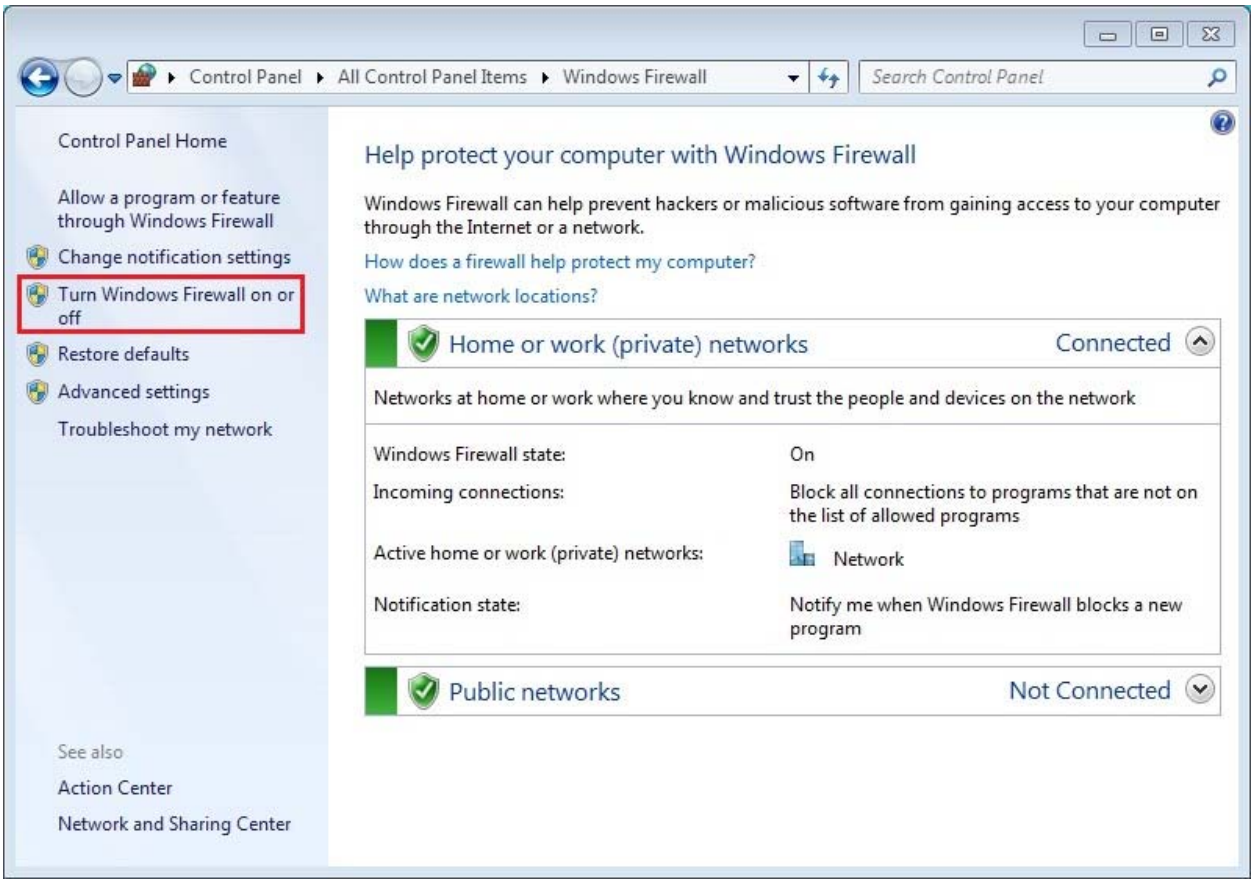
✓ إعداد جد ران الحماية

تعمل جدران الحماية كخط دفاعي لمنع التهديدات من دخول نظامك، فهي تخلق حاجزًا بين جهازك والإنترنت عن طريق إغلاق المنافذ ports أمام الاتصال. يمكن أن يساعد ذلك في منع دخول البرامج الضارّة ويمكن أن يوقف تسرّب البيانات من جهازك.

عادةً ما يحتوي نظام تشغيل جهازك على جدار حماية مدمج. بالإضافة إلى أنّ جدران الحماية المادية مدمجة في العديد من أجهزة التوجيه Router. فقط تأكّد من تمكين لك.

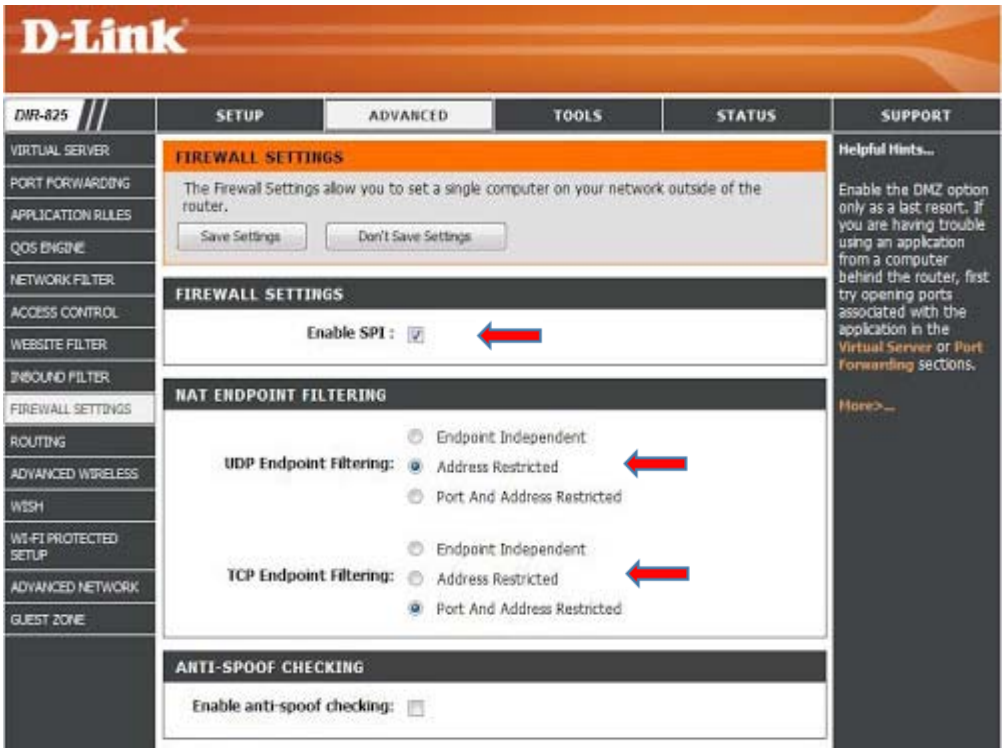
- في نظام التشغيل Windows 10 كما الموضّح في الشكل 1:

control panel > system and security > windows defender firewall



الشكل 1

- في جهاز التوجيه Router (مثلاً Router D_Link) كما الموضّح في الشكل 2.



الشكل 2

إذا لم يكن لديك جدار حماية مدمج أو تبحث عن بعض الحماية الإضافية، فهناك الكثير من جدران الحماية المستقلة.

✓ تنصيب تطبيقات مكافحة البرمجيات الخبيثة والتأكّد من تحديثها بشكلٍ مستمر ودائم.

على الرغم من أنّ جدار الحماية يمكن أن يساعد، إلا أنّه لا مفرّ من أنّ التهديدات يمكن أن تمرّ. يمكن أن يعمل برنامج مكافحة الفيروسات الجيد كخط الدفاع التالي من خلال اكتشاف البرامج الضارة المعروفة وحظرها، وفي حال تمكّنت البرمجيّات الخبيثة من العثور على طريقها إلى جهازك، فقد تتمكّن برامج مكافحة الفيروسات من اكتشافه وإزالته في بعض الحالات، أو على الأقل تنبيهك.

✓ تأمين جهاز التوجيه المنزلي

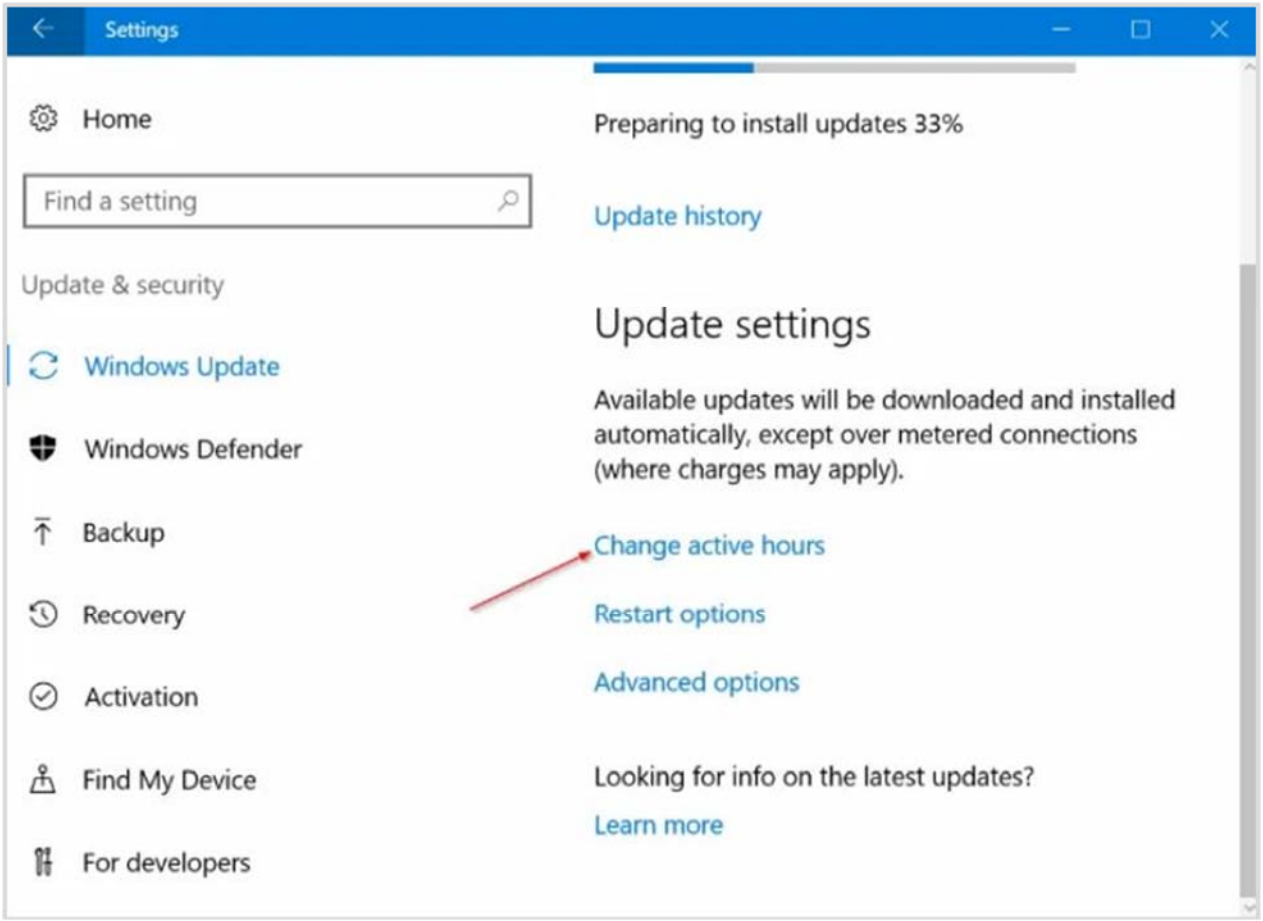
- بتغيير جميع كلمات المرور لجهاز التوجيه الخاص بك بشكل دوري واعتماد كلمات مرور معقدة.
- التأكد من تثبيت التحديثات بحيث يمكن تصحيح الثغرات الأمنية.
- يجب ضبط التشفير على WPA2 أو WPA3 أو أعلى مستوى تشفير متوفر.

- تقييد حركة المرور الواردة والصادرة.
- إيقاف تشغيل WPS.
- التحكم بالسماح للأجهزة بالاتصال من خلال العنوان الفيزيائي MAC ADDRESS حيث لا يمكن لأي جهاز أن يتصل بالموجه دون موافقتك.

✓ **تثبيت تحديثات برامج الجهاز والتطبيقات الأخرى بشكل دائم ومستمر**

قد يكون هذا مصدر إزعاج إلا أنّه غالباً ما تتضمّن التحديثات تصحيحات للثغرات الأمنية التي تمّ الكشف عنها.

في العديد من الحالات، يمكنك تعيين تحديثات للتشغيل تلقائيًا، غالبًا أثناء النوم، لذلك لا داعي للقلق بشأن وقت التوقف عن العمل ويتمّ ذلك في نظام التشغيل windows 10 كما الموضّح في الشكل 3:



الشكل 3

✓ الحرص على أخذ نسخة احتياطية للبيانات Back up Data

يحتمل فقدان البيانات بعديد من الحالات، بما في ذلك الخطأ البشري أو التلف المادي للأجهزة أو الهجوم السيبراني حيث يمكن أن تقوم برمجيات الفدية وأنواع أخرى من البرمجيات الضارة بمسح أنظمة كاملة دون أن تتاح لك فرصة اكتشاف مثل هذه البرمجيات الخبيثة.

قد لا تلبي خدمات النسخ الاحتياطي السحابي الخارجية متطلبات العمل والحفاظ على البيانات والخصوصية وذلك بحسب درجة تصنيف هذه البيانات، ومن الممكن أخذ نسخ احتياطية عن البيانات المهمة على أجهزة تخزين خارجية وتجنب تخزينها على سطح المكتب أو ضمن القسم الأساسي C بالنسبة لنظام التشغيل windows.

✓ الحذر عند استخدام وسائل الاتصال عن بعد

الكثير من المؤسسات ستسمح للموظفين بالوصول إلى عملهم عبر برتوكولات الاتصال بسطح المكتب البعيد وبذلك يكونون أكثر عرضة للهجمات حيث تبيّن وجود عدد من الثغرات الأمنية في الأداة الأكثر شيوعاً لاستخدامها وهي Remote Desktop Protocols (RDPs) ولا ننصح باستخدامها حيث تم اكتشاف عدة حالات اختراق مقترنة بخدمة سطح المكتب البعيد.

✓ البحث عن رسائل ومواقع التصيّد الاحتيالي

يستخدم المهاجمون رسائل البريد الإلكتروني المخادعة، وكذلك رسائل البريد الصوتي (vishing) والرسائل النصية (smishing) "للتصيد الاحتيالي" للحصول على معلومات يستخدمونها عادةً في هجمات التصيد الاحتيالي (phishing attacks) بهدف الاحتيال والاستيلاء على الحساب.

مع تفشي فيروس كورونا سيزداد عدد هذه الهجمات مع ارتفاع عدد الأشخاص الذين يعملون من منازلهم في محاولة لسرقة معلوماتهم الشخصية أو الوصول إلى حسابات الشركة.

لتحديد رسالة بريد إلكتروني فيما إذا كانت حقيقة أم مخادعة:

- تحقق من عنوان البريد الإلكتروني للمرسل بحثًا عن أخطاء إملائية وابحث عن القواعد النحوية الضعيفة في سطر الموضوع ونص البريد الإلكتروني.

- مرر مؤشر الماوس فوق الروابط لمشاهدة عنوان URL ولا تنقر على الروابط أو المرفقات إلا إذا كنت تثق في المرسل بنسبة 100%. إذا كان لديك أي شك، فاتّصل بالمرسل المزعوم باستخدام رقم هاتف أو عنوان بريد إلكتروني تجده في مكان آخر غير البريد الإلكتروني المريب.
- إذا قمت بالنقر فوق ارتباط وانتهى بك الأمر على موقع ذي مظهر شرعي، فتأكّد من التحقق من مصداقيته قبل إدخال أي معلومات.

تتضمن العلامات الشائعة لموقع التصيد الاحتيالي:

- عدم وجود رمز قفل HTTPS (على الرغم من أنّ مواقع التصيد تحتوي على شهادات SSL بشكل متزايد).
- أسماء النطاقات تحتوي على أخطاء إملائية، وقواعد هجاء وقواعد نحوية ضعيفة.
- عدم وجود صفحة "حول"، ومعلومات الاتصال مفقودة.
- وجود حقول الإدخال الخاصة بسرقة الحساب فقط وإذا مررت الفأرة فوق بقية الروابط لن يظهر لك أي رابط في أسفل الزاوية اليسرى للمتصفح.

وفي حال عدم تمكنك من كشف الرابط الاحتيالي يمكنك التواصل مع مركز أمن المعلومات للمساعدة.

✓ الحذر من الحيل عند البحث عن عمل للقيام به من المنزل

بالإضافة إلى هجمات التصيد الاحتيالي، من المحتمل أن نشهد زيادة في عمليات الاحتيال تستغل الحاجة للعمل من المنزل وتسوق على أنّها فرص عمل مشروعة وجذّابة من المنزل. الكثير من هذه المواقع يطلب معلومات شخصية ويطلب حسابك لتحويل دفعات مسبقة قبل بدء العمل.

لذلك عندما تبحث عن عمل لحسابك الخاص فاستخدم المواقع ذات السمعة الطيبة التي توفّر الحماية لكلٍّ من العملاء والمستقلين ولا تشارك المعلومات الشخصية أبدًا مع عميل لم تبحث عنه جيدًا.

✓ استخدام وسائل اتّصال مشفّرة

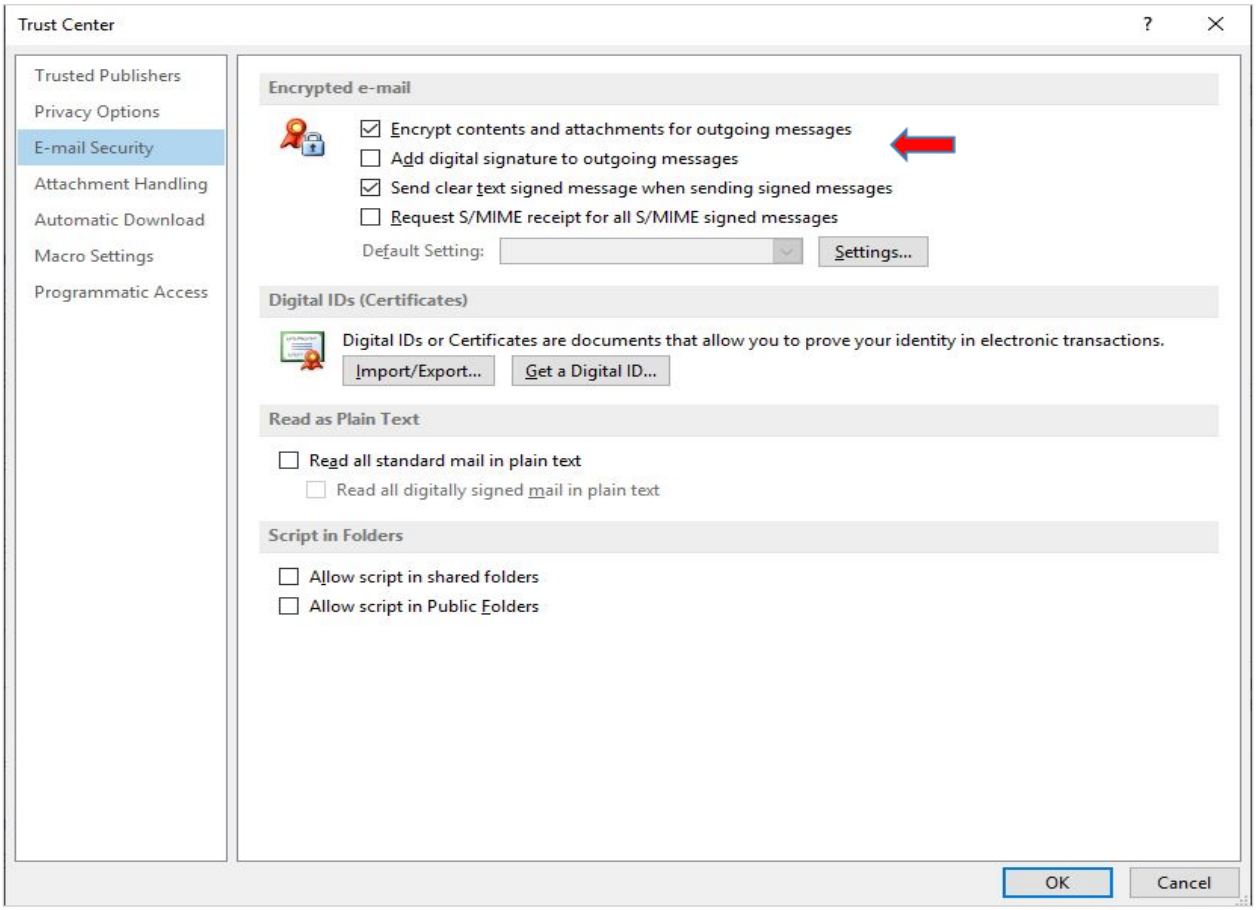
هناك أوقات تحتاج فيها إلى التواصل مع زملائك في العمل وقد تضّطر إلى تبادل معلومات حساسة، إذا كانت شركتك لا توفّر لك بالفعل طرق اتّصال آمنة، هنا يكون لديك عدّة خيارات للحماية:

- استخدام خدمات المراسلة الرئيسية والتي تتميّز بتشفير الرسائل من بداية الإرسال وحتى التسليم بشكل افتراضي مثل Signal و WhatsApp و Telegram.

- استخدام البريد الالكتروني مثل gmail ، outlook بعد تفعيل ميزة التشفير

مثلاً في برنامج outlook بعد أن يتمّ فتحه كما الموضّح في الشكل 4:

File > Options > Trust Center > Trust Center Settings > Email Security



الشكل 4

✓ قفل الجهاز عند الانتهاء من العمل

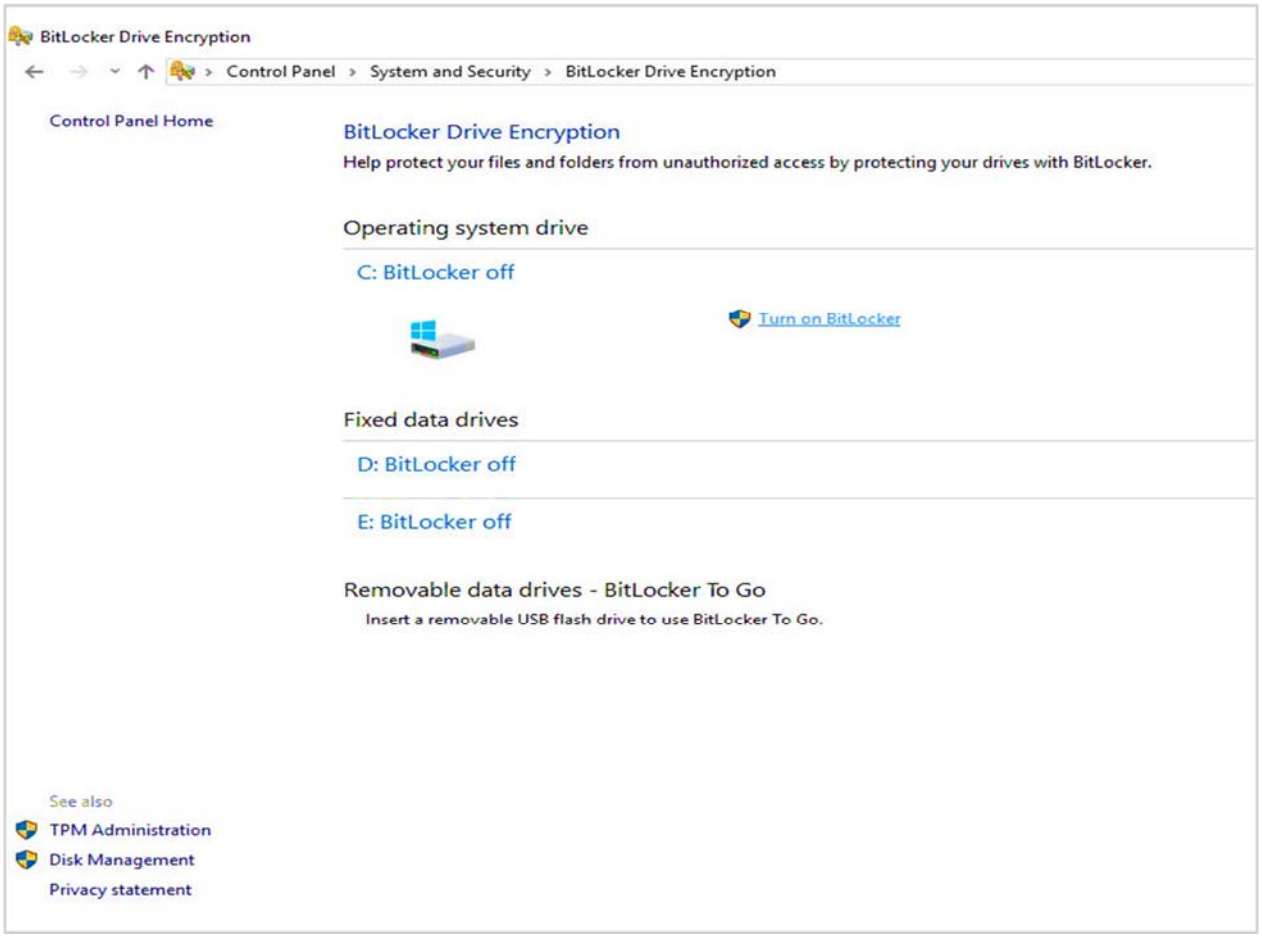
إذا كنت تعيش مع أشخاص لا يمكنك مشاركة معلومات العمل معهم، فمن المهمّ الحفاظ على أمان جهازك.

إذا كنت تبحث عن مزيد من الحماية، فيمكنك استخدام أداة تشفير قرص إضافية كاملة مثل أداة BitLocker المثبتة في نظام التشغيل ويندوز ومن ميزات مثل هذه الأدوات:

- إنشاء قرص مشفّر افتراضي داخل ملف وتثبيته كقرص حقيقي.

- تشفير جهاز تخزين مثل محرك أقراص USB المحمول أو محرك الأقراص الثابتة.
- يكون التشفير أوتوماتيكيا وسريعاً حيث يتمّ تشفير البيانات بالتوازي مع كتابتها كما يمكن قراءة البيانات بسرعة كما لو لم يتمّ تشفير محرك الأقراص.
- في حالة إجبار الضحية على الكشف عن كلمة المرور فإنّها توفّر وسيلة لإخفاء البيانات.

يمكن تفعيل أداة BitLocker في نظام التشغيل windows 10 كما الموضح في الشكل 5:



الشكل 5

المصادر

- https://www.comparitech.com/blog/information-security/security-remote-working/
- https://www.zdnet.com/article/covid-19-with-everyone-working-from-home-vpn-security-has-now-become-paramount/
- https://www.comparitech.com/blog/vpn-privacy/how-to-encrypt-email/