الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

المركز الوطني الإرشادي
للأمن السيبراني
SAUDI CERT

دليل إرشادي للجمعيات الخيرية والجهات غير الربحية

لجوانب الأمن السيبراني في العمل عن بُعد

إشارة المشاركة: أبيض
تصنيف الوثيقة: متاح

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل او خارج المنشأة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

جدول المحتويات

مقدمة

انطلاقًا من إدراك المملكة العربية السعودية لأهمية مواكبة التغيرات الحثيثة الناجمة عن مستجدات هذا العصر وتطوراته، وترجمةً لنهج خادم الحرمين الشريفين الملك سلمان بن عبد العزيز وسمو ولي العهد حفظهم الله في قيادة بلادنا لتكون نموذجًا ناجحًا ورائدًا في العالم على كافة الأصعدة، ولرؤية المملكة ٢٠٣٠ التي جعلت التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية ضمن مستهدفاتها، واستشعارًا لأهمية البيانات والأنظمة التقنية والبنى التحتية الحساسة وارتباطها بالمصالح الوطنية، وأهمية حمايتها من أي تهديدات أو مخاطر يشهدها الفضاء السيبراني، فقد جاء تأسيس الهيئة الوطنية للأمن السيبراني وارتباطها بالملك -حفظه الله- وذلك وفق الأمر الملكي الكريم بالموافقة على تنظيمها بتاريخ ١٤٣٩/٢/١١هـ لتكون الهيئة هي الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه، وتهدف إلى تعزيزه؛ حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية.

تشهد المملكة اليوم تحولًا واسع النطاق إلى استخدام الفضاء السيبراني والاستفادة مما يوفره من إمكانات للعمل والتعلم عن بُعد، وبالأخص بعد تأثيرات جائحة كورونا، حيث استدعت الحاجة للعمل عن بعد في العديد من الجهات ومنها الجمعيات الخيرية والجهات غير الربحية. وهذا التحول من شأنه أن يثري الأعمال الخيرية والتطوعية وخطط التحول في المملكة بمزيد من الخدمات والمميزات التي لم تكن موجودة من قبل مع إتاحة كافة تلك المميزات في جميع مدن وقرى المملكة. وكما هو معروف، فإن أي تحول بهذا الحجم يتضمن عددًا من المخاطر التي لا بد من مراعاتها لتجنب السلبيات المحتملة سواء لخصوصية الموظف، أو لأمن وسلامة خصوصية الجمعيات الخيرية والجهات غير الربحية، واستمرارية أعمالها وخدماتها.

وحيث جاء ضمن اختصاصات ومهام الهيئة «رفع مستوى الوعي بالأمن السيبراني». وفي ظل ما تمر به المملكة اليوم من تحديات عاجلة وفرص نادرة في باب التحول إلى العمل الإلكتروني عن بُعد على نطاق واسع في القطاعين الخاص والعام، يأتي هذا الدليل من الهيئة الوطنية للأمن السيبراني من أجل عون الجمعيات الخيرية والجهات غير الربحية على التبني الأمثل لتلك التقنية في بيئة تعزز من مستوى الأمن السيبراني لديهم بإذن الله تعالى.

سيفتتح هذا الدليل بتعريف لأبرز فئات وتصنيفات منصات العمل للجمعيات الخيرية والجهات غير الربحية والواجب معرفة الفروقات بينها ليتمكن الموظف من تحصينها بفاعلية. ويحتوي الدليل على سبع خطوات عملية متسلسلة للتحصين الأمني لبيئة العمل عن بُعد في تلك الجهات، وذلك على النحو التالي:

١. نبذة عامة عن كيفية مراجعة وتحصين شبكة المنزل ضد الاختراقات.

٢. أبرز الإجراءات الوقائية الواجب مراعاتها لتحصين حاسبك وأجهزتك الذكية.

٣. إرشادات أمنية حول أساسيات تجهيز وتخصيص مكان في المنزل للعمل عن بُعد.

٤. منصات عملك الجديدة في ظل أهم الجوانب الأمنية الواجب مراعاتها.

٥. أبرز الاحتياطات الأمنية الواجب مراعاتها لتحصين منصة العمل التعاوني والتنسيق عن بُعد.

٦. ملخص لأبرز الاحتياطات الأمنية الواجب مراعاتها من قبل الموظف لتحصين أنظمة العمل الداخلية للجمعيات الخيرية والجهات غير الربحية لعدم عرضها للاختراقات.

٧. أبرز الإجراءات الأمنية للعاملين عن بُعد في الجمعيات الخيرية والجهات غير الربحية خلال التنقل أو السفر.

يحتوي ختام هذا الدليل على روابط وإرشادات هامة ذات علاقة بالعمل عن بُعد والتي تسهّل للموظف طلب المساعدة أو تجنب الوقوع في المحاذير النظامية.

ملخص

عزيزي الموظف ، عزيزتي الموظفة في الجمعيات الخيرية والجهات غير الربحية

وعيك هو سلاحك الذي سيساهم في حماية معلوماتك وأجهزتك وخصوصيتك أثناء العمل عن بعد.

لذا يطلق **المركز الوطني الإرشادي للأمن السيبراني** دليلاً للجمعيات الخيرية والجهات غير الربحية مشتملاً على ما يلي:

تمهيد

الوطن مع الموظف في سفينة التحوّل

تشهد المملكة العربية السعودية اليوم تحولاً تاريخياً شاملا على تقنيات العمل عن بُعد. ومحور ذلك التحوّل هو الموظف، في الجمعيات الخيرية والجهات غير الربحية. وهذا يستوجب علينا جميعاً التكاتف لتوعية أنفسنا وزملائنا بالعمل بأفضل الممارسات والاحتياطات الأمنية التي من شأنها حماية خصوصيتنا وبيانات مكان عملنا الحساسة بفاعلية لنجمع بين الاستفادة المثلى من هذه التقنيات المتميزة مع تجنب مخاطرها ومحاذيرها.

أساليب حديثة والكثير من الخدمات ... بخطوات واعية وحذرة

التقنية اليوم بين يديك.

- تجتمع مع من تشاء بالصوت والصورة في أي موقع أو وقت تختاره.
- تشارك وثائق مشاريعك إلكترونياً مع زملائك في الجمعيات الخيرية والجهات غير الربحية بأي ساعة تشاء.
- تنجز كافة مهامك المالية والإدارية الرسمية عن بُعد.
- تدير المهام المعقدة والمتشعبة بأدوات إلكترونية تبسطها وتعينك على أدائها بجودة واحترافية.

كل ذلك وأكثر بانتظارك في منصات تقنيات وطنك الحديثة للعمل عن بُعد.

يمكن حصر أبرز المخاطر الأمنية للعمل عن بُعد بالفئات الأساسية التالية:

١. **الإزعاج:** مثل إرباك الاجتماعات وإضاعة أوقات المشاركين أو خدش الحياء والقيم. ومن نماذجه الواقعية حالات حصل معها اقتحام لغرف الاجتماعات من قبل أشخاص غير مصرحين مع عرضهم لمشاهد إباحية على الجميع.

٢. **السرية:** مثل التصنت على الاجتماعات وكشف أسرار العمل. ومن نماذجه الواقعية ما حدث من كشف لتسجيلات اجتماعات حساسة وخاصة مع تمكين أناس غرباء من مشاهدتها.

٣. **الخصوصية:** مثل الاتجار بمعلومات الموظف الشخصية واهتماماته. ومن نماذجه الواقعية حصد الشركة القائمة على منصات العمل عن بُعد للبيانات الخاصة للمستخدمين وسماتهم الأساسية واهتماماتهم وتمكين شركات تجارية من الحصول على تلك البيانات.

٤. **الاختراق:** مثل فتح ثغرات جديدة على حاسبات الموظفين بسبب تبني هذه القنوات الإلكترونية الجديدة. ومن نماذجه الواقعية التقاط الروابط المستخدمة للدعوة إلى اجتماع افتراضي وسوء استغلالها من أجل الحصول على الصلاحيات الإلكترونية لحاسبات الموظفين المشاركين في ذلك الاجتماع واختراقها.

إن وعيك وحرصك كموظف في الجمعيات الخيرية والجهات غير الربحية – بعد توفيق الله - هما سبيلك إلى التقليل من إمكانية التعرض لأحد تلك المخاطر وتحصين أسرار جهة عملك وحماية معلوماتك وجهازك وخصوصيتك وخصوصية بيتك. فلنبدأ معاً رحلة التبني الحكيم الواعي لتقنيات العمل عن بُعد في بيئة آمنة، بإذن الله.

التصنيفات العامة لخدمات العمل الإلكترونية: رحلة قصيرة للتعرف على بيئة الجمعيات الخيرية والجهات غير الربحية الجديدة

قبل أن نتمكن من حماية أنفسنا وجهات عملنا من المخاطر الإلكترونية الأمنية الجديدة المصاحبة لبيئات العمل عن بُعد، لا بد أولاً أن نكوّن نظرة شمولية لمنظومة العمل عن بُعد وأبرز سماته.

إن منظومة العمل عن بُعد تتألف من عدد غفير من الخدمات الإلكترونية المتفرقة والتكاملية في وطننا اليوم. وحتى يتسنى تقديم إرشادات عملية لكيفية تحصينها أمنيًا من المهم أولًا الاتفاق على بعض التعريفات الأساسية التي سوف يرتكز عليها هذا الدليل. يُعرِّف هذا الجزء الأقسام الرئيسة للخدمات الإلكترونية للعمل عن بُعد، والتي يمكن تبويبها على وجه العموم كما يلي:

١. أنظمة العمل الداخلية: وهي الخدمات الإلكترونية المخصصة لحفظ وإدارة بيانات الجمعيات الخيرية والجهات غير الربحية الداخلية وملكيتها الفكرية السرية ولإدارة أعمال منسوبيها، ومن أبرزها:

أ. النظام الإلكتروني للشؤون المالية والإدارية للجمعيات الخيرية والجهات غير الربحية والمعد لإدارة إجازات الموظف، وعهده، وتاريخه الوظيفي، وتفاصيل مرتبه وبدلاته، ومشتريات ومستودعات الجمعيات الخيرية والجهات غير الربحية، وما شابهها.

ب. النظام الإلكتروني المخصص لإدارة المراسلات والخطابات الرسمية.

ت. الأنظمة الإلكترونية الداخلية المتخصصة المعدّة لخصوصية طبيعة عمل الجمعيات الخيرية والجهات غير الربحية، مثل أنظمة جمع التبرعات و أنظمة التطوع وغيرها من الأنظمة.

ث. البوابات الإلكترونية الداخلية المعدة للموظفين لجمع كافة الخدمات الداخلية لكفاءة خدمة الموظفين.

ج. الخدمات الإلكترونية الأساسية مثل البريد الإلكتروني الجمعيات الخيرية والجهات غير الربحية أو أنظمة حفظ وتبادل الملفات الداخلية والمجلدات الشبكية المشتركة الداخلية.

علماً بأن الجمعيات الخيرية والجهات غير الربحية تتيح لمنسوبيها الوصول لهذه الخدمات من خارج الجهة من خلال قنوات آمنة ومشفرّة معدة خصيصًا لذلك وتسمى «**الشبكات الخاصة الافتراضية VPN**». وأن المهمة الأساسية لهذه القنوات هي مد خط اتصال مشفّر بين حاسبك المنزلي ومركز معلومات الجمعيات الخيرية والجهات غير الربحية يتم من خلالها إتاحة وصولك إلى تلك الخدمات الداخلية بشفافية وكأنك متواجد بداخل مكتبك ولكن بصفة تمنع التصنّت أو التجسس على أعمالك من قبل أي طرف خارجي آخر.

٢. منصّات العمل التعاوني والتنسيق عن بُعد: منظومة الخدمات الإلكترونية التي تنظم كافة أعمال التنسيق والتعاون بين فرق العمل والزملاء العاملين بداخل جمعية خيرية أو جهة غير ربحية أو المتعاونين في مهام مشتركة بين أكثر من جهة. ومن أبرز الخدمات التابعة لهذا الباب ما يلي:

أ. خدمات تنظيم وإدارة الاجتماعات الحيّة عن بُعد وهي عبارة عن باقة من الخدمات، منها:

- اجتماعات بالصوت والصورة لمناقشة قضايا عمل مشتركة بأريحية وخصوصية.
- خدمات التحضير لتلك الاجتماعات مثل إرسال جداول الأعمال والمرفقات، أو تنظيم الوقت وأعمال التصويت على بنود الاجتماع خلال عقده وتوثيق الحضور وأعمال التنظيم بعد انتهاء الاجتماع لإعداد المحاضر وتوزيعها على سبيل المثال.
- خدمات التعاون الحي بين أعضاء مجموعة عمل لتأليف ومراجعة الوثائق عن بُعد.

ب. خدمات الدردشة الحيّة: وتشمل تبادل النصوص القصيرة بين أفراد أو مجموعات عمل في أي وقت وأي مكان بغرض التنسيق والإحاطة للجميع، مع إمكانية دعم تلك الرسائل بمرفقات مناسبة مثل صور، أو مواقع جغرافية، أو مستندات عمل، أو معلومات اتصال لأفراد.

ت. **خدمات إدارة المهام:** وهذه الخدمة تسمح بتقسيم برامج العمل الكبيرة إلى مبادرات، ثم إلى مشاريع فمهام، بدرجاتٍ متتالية من الدقّة والتفصيل، بحيث يتم تخصيص ما تسمى «بطاقة» لكل مهمة صغيرة، ثم يتم جمع تلك البطاقات في «مجموعات» تمثل المشاريع، وهكذا. ثم يتم إسناد تلك البطاقات إلى أفراد أو مجموعات عمل مع تحديد تواريخ الإنجاز المطلوبة، ومع باقة من الخدمات المساندة الإضافية. تساعد هذه الخدمة في عمومها الجمعيات الخيرية والجهات غير الربحية والمدراء وفرق العمل على تنسيق وتنظيم أعمالهم بما يخدم النظرة الشمولية والأهداف والمؤشرات العامة للجهة بجودة وكفاءة.

ث. **خدمات تخزين ومشاركة الملفات:** وهذه الخدمة الإلكترونية تُعنى بحفظ المستندات المشتركة في مستودعات إلكترونية شبكية عامة مع إدارة صلاحيات الوصول إليها من قبل أعداد متفاوتة من الموظفين حسب الحاجة، ومع السماح بتشفيرها وإدارة إصداراتها بكفاءة وجودة.

تسرد هذه الوثيقة جملة من التوصيات الأمنية لهاتين الفئتين الرئيستين من الخدمات الإلكترونية، وهي «أنظمة العمل الداخلية» و «منصات العمل التعاوني والتنسيق عن بُعد».

الخطوة الأولى:
خطوات عملية لتحصين شبكة «مكتبك المنزلي»

نبدأ رحلة العمل عن بعد بتجهيز شبكة المنزل (الواي-فاي) وتحصين بيئة المعلومات في منزلك وسد ثغراتها الأمنية. وأهم خطوة لذلك هي مراجعة إعدادات موجّه الشبكة (الراوتر) لمنزلك. استعن بإرشادات جهازك وطبّق الإعدادات التالية:

١. فعّل الاتصالات اللاسلكية المشفرة من خلال تفعيل خاصية **WPA3**، أو **WPA2** في حال عدم توفره. وإطفاء خاصية **WAP** الضعيفة.

٢. أطفئ خاصية إدارة الموجه **(الراوتر)** عن بُعد **(remote management)** لمنع الآخرين من تغيير إعدادات الجهاز من خارج المنزل.

٣. إذا كانت كلمة السر المصنعية المعدّة لإدارة إعدادات الموجه ضعيفة **(مثل admin أو password)**، غيّرها لكلمة سر قوية تحتوي على أرقام ورموز وحروف كبيرة وصغيرة. وإذا كانت كلمة المرور مطبوعة على الجهاز وتبدو معقّدة ويصعب تذكّرها، فيمكنك تركها.

٤. شغّل خاصية الإدارة المشفّرة للموجّه الشبكي **(https)** - بدلاً من **(http)** - لضمان عدم قدرة الآخرين على التجسس عليك وأنت تغيّر إعدادات موجه منزلك، ومن ثم اختراقه.

٥. اشتر موجهات رئيسة منزلية تحتوي على جدار حماية، مع تشغيل ذلك الجدار.

٦. احرص على تحميل تحديثات المصنع للموجّه المنزلي بصفة دورية لإغلاق الثغرات الأمنية الجديدة المكتشفة أولاً بأول.

٧. غيّر العنوان الافتراضي لإدارة الجهاز إن سمحت الإعدادات بذلك (مثل تغييره من **192.168.1.1** إلى **192.168.50.1**).

٨. أطفئ خواص **WPS** و **UPnP** حيث ثبت سهولة اختراقهما.

٩. فعّل «**شبكة الضيوف**» ولا تسمح إلّا لأهل بيتك الموثوقين باستخدام شبكة الواي-فاي الأساسية، وذلك لمنع الضيوف، أو غيرهم، من الوصول إلى موارد وخدمات شبكتك المنزلية، مثل الكاميرات المنزلية، أو الأجهزة الذكية المنزلية، أو أنظمة التخزين المشتركة المنزلية، أو غيرها.

١٠. غيّر اسم شبكة **الواي-فاي** المصنعية إلى كلمة أخرى من اختيارك لمنع المخترقين من سهولة التعرّف على نوع وموديل جهازك، ومن ثم اختراقه.

١١. ضع الجهاز في منتصف المنزل قدر المستطاع للحد من قدرة الآخرين على التسلل إليه من خارج منزلك.

الخطوة الثانية:
أفضل الممارسات لتحصين حاسبك الشخصي ضد المخاطر الأمنية

بعد أن فرغنا من تطبيق أفضل الممارسات لحماية شبكة منزلك، ننتقل الآن إلى إعدادات حاسبك الشخصي أو جهازك الذكي:

١. أكبر ثغرة أمنية يمكنك أن تفتحها على جهازك هي استخدامك لنظام تشغيل **غير أصلي** أو لبرامج **غير أصلية** مهما كان مصدرها لأنها على الأغلب تحوي مكوّنات غير آمنة ومخاطر ولا يمكن إصلاحها بسهولة.

تحوي معظم الأجهزة المتوفرة في السوق الوطني اليوم نسخ أصلية من نظام التشغيل وهذا يوفر قدرًا أعلى من الأمان لجهازك.
عموماً فإن كافة الأجهزة التي يتم صرفها من قبل الجمعيات الخيرية والجهات غير الربحية لا تستخدم إلّا برامج أصلية. فاحرص على تنفيذ كافة أعمالك من خلال تلك الأجهزة الرسمية فقط قدر المستطاع.

٢. الآن وقد ضمنت أن كافة برامجك أصلية، أصبح من حقك تحميل كافة التحديثات الدورية المصنعية لنظام التشغيل وبقية البرامج والتطبيقات التابعة لجهازك، لسد الثغرات الأمنية الجديدة المكتشفة أولاً بأول. على الأغلب ستتولى جهة عملك تنفيذ تلك التحديثات آلياً دون تدخلك لو كان جهازك تابعاً لجهة عملك، لكن إن كان جهازًا خاصًا فاحرص على الاستفادة من كافة تلك التحديثات، وفعّل التحديث التلقائي.

٣. فعّل خاصية مكافحة الفيروسات والحماية في جهازك إن كانت متوفرة. وإن لم تكن متوفرة، اشتر أحد برامج الحماية الشاملة الشهرية التي تحتوي على خواص جدار حماية وبرنامج مكافحة فيروسات قوي، واحرص على اتّباع تعليماته لضمان تحديثه آلياً لمواكبة أحدث التهديدات المكتشفة.

٤. أطفئ خواص «المشاركة الشبكية» (**file and network sharing**) في الجهاز في حال عدم الاحتياج إليها للحد من فرص دخول الآخرين إلى جهازك.

٥. أطفئ كافة خدمات الاتصالات غير الضرورية وشغّلها فقط عند الضرورة، مثل **WiFi**، و **NFC**، و **Bluetooth**، و **Hotspot**، فهي تستهلك بطارية جهازك و قد تفتح ثغرات يمكن للمخترقين استغلالها.

٦. احرص على تشفير الأقراص الداخلية لجهازك لحماية بياناتك في حال سرقته، ويمكن تحقيق ذلك من خلال عدة وسائل مثل برنامج **BitLocker** المتوفر بداخل أنظمة مايكروسوفت ويندوز، أو **VeraCrypt** المجاني، أو غيرهما.

٧. أخيراً، إن كانت الجمعية الخيرية أو الجهة غير الربحية تملك حاسبك المستخدم للعمل، تأكّد من مراقبة عمليات التحديث لنظام التشغيل ولبرنامج مكافحة الفيروسات وأنت خارج شبكة عملك للتأكد من أنهما يعملان بسلامة على الدوام، وبادر بإبلاغ مكتب الدعم الفني في الجمعية الخيرية أو الجهة غير الربحية فور ظهور أي خطأ في عمليات التحديث خارج شبكتها.

الخطوة الثالثة:
تجهيز بيئة «مكتبك المنزلي»

إنّ كثرة التنقل والتغيير داخل المنزل وبين الأجهزة من الأسباب التي قد تؤدي إلى انتهاك خصوصية الموظف وخصوصية بيته أو إلى مشاكل في الأداء. ولتجنّب ذلك احرص على ما يلي:

١. خصّص مكاناً محددًا في منزلك لأداء أعمالك عن بُعد.

٢. يفضّل استخدام حاسب مقدّم من الجمعية الخيرية أو الجهة غير الربحية يحتوي على إعدادات أمان عالية. وفي حال استخدام جهاز شخصي حاول أن تخصص جهازاً للعمل عن بُعد فقط، وتجنّب تغييره باستمرار.

٣. تأكّد من تفعيل خاصيّة «شاشة التوقف» لجهازك لمنع سوء استخدامه بهويتك واسمك في حال غيابك عنه.

٤. تجنّب السماح للآخرين باستخدام الحاسب الشخصي المعد للعمل عن بُعد إلا للضرورة وتحت رقابتك.

٥. ضع حاسبك بوضعية تحفظ خصوصية منزلك في حال فتحت كاميرته أو ميكرفونه.

٦. استعن بسماعات أذن عالية الجودة لحفظ خصوصيتك وقت الاجتماعات الافتراضية ولتجنّب الإزعاج، وتأكّد من شحنها في نهاية كل يوم إن كانت لاسلكية.

٧. بلّغ عائلتك بجدول أوقات عملك، ويفضّل طباعة تلك الأوقات بوضوح على باب مكتبك المنزلي لضمان عدم الإحراج أو الإزعاج خلال تلك الأوقات.

الخطوة الرابعة:
تسلّح بالعلم

من طبعنا جميعاً عند تبني تقنية جديدة أن نتجنّب قراءة التعليمات وننطلق فوراً إلى استخدامها، إلا أن تلك العادة كثيراً ما تؤدي إلى سلبيتين:

١. تفويت المزايا المفيدة التي تسهّل عملنا.

٢. ربما نفتح على أنفسنا ثغرات أمنية بسبب عدم التفرّغ لضبط المميزات الأمنية لتلك التقنية.

وبصفة مشابهة، عندما تتحول كموظف من المكتب التقليدي إلى المكتب الافتراضي الإلكتروني، ربما ساقك الحماس إلى استخدام المنصة فورًا بدون التفرّغ أولاً للتعرف على مميزاتها ومحاذيرها بالتفصيل. وقد يؤدّي هذا إلى مخاطر على سرية وخصوصية معلوماتك الشخصية. ويمكنك تجنب ذلك بسهولة كما يلي:

١. قبل البدء باستخدام أي منصة عمل جديدة، من المناسب لك قراءة أدلة الاستخدام المعدّة لك من قبل مكان عملك، علماً بأن جل الجمعيات الخيرية والجهات غير الربحية قد خصّصت باقة من الخدمات لدعم تحول منسوبيها، تتراوح بين دعم حي عبر مكاتب الدعم الفني، مقاطع فيديو قصيرة إرشادية وإرشادات مطبوعة، فاحرص على الاستفادة منها جميعًا.

٢. الاستفادة من الموارد الخارجية لتلك المنصات والتي تجدها في العادة في الموقع الإلكتروني للشركات المصنّعة لها حيث ستجد تعليمات مفصّلة عن كامل مميزاتها وكيفية الاستفادة منها وكيفية ضبطها حسب حاجتك. ومن المفيد أن تزور مواقع عالمية للمقاطع التعليمية المصورة مثل يوتيوب، حيث ستجد مقاطع من الشركة المصنّعة لتلك المنصة ومن مدربين ومستخدمين آخرين عن كيفية الاستفادة من مميزات منصات الأعمال تلك وكيفية ضبطها لخدمتك ولحفظ خصوصيتك ولتسهيل أعمالك.

٣. لا تنس زيارة المواقع الوطنية المعدة لتوعيتك وحمايتك من مخاطر أمن المعلومات – مثل المركز الوطني الإرشادي للأمن السيبراني – لتطّلع على ما لديها من نشرات حول منصة العمل عن بُعد المستخدمة من قبل الجمعية الخيرية أو الجهة غير الربحية، ولتشترك في خدمة التنبيهات الأمنية المقدّمة من قبلها.

٤. من الطبيعي أن تلعب اللغة الأجنبية والتعقيد التقني أدواراً رئيسة في مدى استفادتك كموظف غير مختص من منصات العمل عن بُعد الحديثة بكفاءة وأمان. لا تخجل إن واجهت صعوبة في فهم بعض المصطلحات الأجنبية أو التقنية واستعن بمكتب الدعم الفني للجمعية الخيرية أو للجهة غير الربحية أو بآخرين من عائلتك أو معارفك لترجمة المصطلحات أو شرحها، وذلك دليل على وعيك.

الخطوة الخامسة:
أفضل الممارسات الأمنية لمنصات العمل التعاوني والتنسيق عن بُعد

عندما تتحول كموظف من بيئة العمل التقليدية إلى بيئة العمل والتنسيق والتعاون الإلكتروني عن بُعد ، ستكتشف مرونة عالية لقنوات التنسيق والاتصال المتاحة لك.

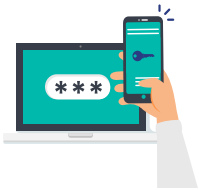
قبل الشروع بالاستفادة من هذه الخدمات الجديدة، اعلم أن الممارسات الأمنية السليمة تنقسم إلى فئتين: فئة ينبغي تطبيقها عند تبني المنصة لأول مرة، وفئة تتم مراعاتها كلما فتحت جلسة جديدة.

تذكر دوماً أن تلتزم بكافة إرشادات وتقنيات مكان عملك الأمنية وألّا تتجاهلها أو تحاول أن تتخطاها، حيث أنها لم توضع إلّا بعد دراسة متعمقة من المختصين لحمايتك وحماية الجمعية الخيرية أو الجهة غير الربحية ضمن أفضل الممارسات الحديثة مع مراعاة أبرز المخاطر الأمنية التقنية المتجددة والتي قد لا تكون على إحاطة بها.

تأمين المنصة قبل أول استخدام:

دقائق من وقتك تستثمرها في إعداد المنصة بالتفصيل قبل أول جلسة تخدمك بدون انقطاع في المستقبل. فرّغ نفسك في المرّة الأولى التي تفتح فيها حسابك في تلك المنصة للتأكّد من ضبطها حسب حاجتك الفعلية دون إفراط أو تفريط، ومن ذلك:

١. غير كلمة السر فور استلام الحساب واتّبع أفضل الممارسات لاختيارها مثل اختيار «جملة سر» بدلاً من كلمة سر، مع تضمينها تشكيلة من الحروف والأرقام والرموز .

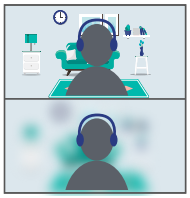


٢. تتيح المنصات الإلكترونية الحديثة من هذه الفئة خاصية «التحقق من الهوية متعدد العناصر» (Multi-Factor Authentication)، احرص على تفعيلها لتحميك من سرقة حساباتك.

٣. تأكد من كامل إعدادات المنصة الجديدة واحدة تلو الأخرى، ومن ضبطها حسب الحاجة لحفظ خصوصيتك وسرية أعمالك.

٤. عند المشاركة بالكاميرا أو الميكروفون أو الدردشة النصية، فإن منصّات تنسيق العمل في الغالب تسمح لك في الجمعية الخيرية أو الجهة غير الربحية باختيار من هو المتلقي، سواء كان زميل عمل محدد، أو فريق عمل متكامل. لذلك وجب عليك الاطّلاع على كيفية ضبط تلك القنوات لضمان عدم إشراكك لأطراف غير مقصودين بدون قصد.

٥. الوثائق والملفات جزء لا يتجزأ من أي عمل جماعي مشترك لفرق العمل. وفي بيئة العمل عن بُعد كثرا ما تتم مراجعتها وتطويرها من خلال مزية «مشاركة سطح المكتب»، بحيث يعرض أحد الأعضاء هذه المستندات على بقية الحضور للمشاركة في مراجعتها وتطويرها بصفة حية. عند مشاركتك لآخرين بمحتويات حاسبك الشخصي بهذه الطريقة، ينبغي عليك التأكد من تحجيم دائرة تلك المشاركة وحصرها بالوثيقة التي تستهدفها والأطراف المعنيين فقط. ولو أردت مشاركة نافذة واحدة من نوافذ سطح مكتب حاسبك الشخصي، فتأكد ألا تفتح كامل سطح مكتب حاسبك للطرف الآخر، وتأكد أيضا من عدم فتحك لنافذة أو أكثر من سطح مكتبك لأطراف آخرين لم تقصدهم. احرص على مراجعة خواص منصتك لتتعلم كيف تفعل ذلك.



٦. عليك أن تراجع خلفية «مكتبك المنزلي» الجديد للتأكد من عدم وجود ما يضر بخصوصية بيتك في حال فتح الكاميرا، علماً بأن بعض أنظمة العمل عن بُعد تتيح للموظف وضع خلفية صناعية من اختياره أو التشويش على الخلفية آليا. قم بتفعيل تلك الخاصة في حال الاحتياج إليها.

٧. كثير من هذه المنصات الحديثة معدّة لتفتح تلقائيا كلما فتحت حاسبك أو جهازك الذكي. وهذا يمثل تهديدًا على خصوصيتك. احرص على ضبطها بحيث لا تفتح إلا بطلب يدوي منك.

٨. في حال عدم احتياجك خلال الجلسة إلى نقل صور حيّة للحضور، عليك التأكد من إغلاق الكاميرا قبل بداية جلسة الاجتماع من خلال مراجعة إعداداتها في منصتك، ثمّ تأكّد بأن نور الكاميرا لا يعمل.

٩. تأكّد من إغلاق الميكروفون قبل بداية جلسة الاجتماع من خلال مراجعة إعداداته في المنصة لحفظ خصوصية منزلك ومنع إزعاج بقيّة الأعضاء إلى أن يحين الوقت المناسب لمشاركتك.

١٠. اعلم أن كثيراً من المنصات الحديثة تسمح لرئيس الجلسة بفتح بعض خدمات حاسبات بقية الموظفين المشاركين بالجلسة وإن كانوا قد أغلقوها من جانبهم مسبقًا، مثل فتح كاميرا الموظفة أو ميكرفونها. ولكن في مجتمعنا الإسلامي المحافظ من المناسب للموظفة أخذ ذلك في الحسبان حتى لا يؤدي إلى تبعات غير مقصودة، ومن أساليب تحقيق ذلك وضع ملصق على الكاميرا.

١١. عند إعداد خواص غرفة اجتماعاتك الافتراضية لأول مرة، قم بضبطها لتجنّب تحميل تسجيلات اجتماعاتك إلى السحابة الإلكترونية الدولية. وفي حالة ضرورة تحميلها:
(١) ضع كلمة سر لحماية تسجيلات تلك الاجتماعات
(٢) راجع إعدادات الخصوصية المرتبطة بها لضمان حصر صلاحيات مشاهدتها على المعنيين فقط، حيث ربما افترضت المنصة ابتداء فتح صلاحيات المشاهدة لأي فرد من حول العالم إن لم يحصرها مدير الجلسة.

١٢. عند إعداد خواص غرفة اجتماعاتك الشخصية، عطّل ميزة «الدخول إلى الاجتماع قبل المضيف» حتى لا يتمكن أحد من الدخول إلى غرفة الاجتماع قبل المضيف نفسه.

١٣. احم غرف الاجتماعات التي تنشئها بكلمات مرور دائمًا، وأقصر توزيعها على المعنيين ومن خلال قنوات مستقلة آمنة، مثل البريد الإلكتروني الخاص بالجمعية الخيرية أو الجهة غير الربحية.

١٤. احرص على عدم تفعيل خاصية «السماح للمشاركين المحذوفين بالعودة إلى الاجتماع» لمنع تكرار الهجوم أو الأذية.

١٥. استعن بخاصية «غرفة الانتظار» التي ينتظر بها جميع المشاركون إلى أن يأذن المضيف بانضمامهم إلى الاجتماع، منعًا لدخول غير المصرحين.

١٦. عطل خاصية «مشاركة الشاشة» لجميع المشاركين إلّا للضرورة، واحصر تلك الصلاحية بك كمضيف وحدك قدر المستطاع.

١٧. عندما تصلك أية رسائل أو تنبيهات بتحديث المنصة (أو إذا ظهرت أمامك نافذة تطلب منك ضغط زر لتحديثها) تجنب الاستجابة واستعض عن ذلك بزيارة الموقع الرسمي للتطبيق أو المتجر الرسمي له، وحدثه يدوًيا من هناك.

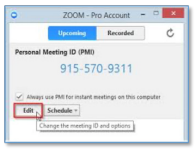
١٨. اطلب من الإدارة القانونية والتقنية في الجمعية الخيرية أو الجهة غير الربحية وضع نص قانوني مناسب في المنصة تحظر الدخول لغير المصرحين مع الإشارة إلى العقوبات المنصوص عليها في نظام مكافحة الجريمة المعلوماتية.

أدر الجلسة باحترافية:

بعد ضبط الإعدادات الأساسية الدائمة لمنصتك، الآن ستنتقل إلى مرحلة الاستفادة الحيّة اليومية منها، وفيما يلي ستجد جملة من التوصيات المهم مراعاتها عند إنشاء أي جلسة اجتماعات جديدة:

١. تجنّب استخدام وتبادل الروابط المباشرة قدر المستطاع واقتصر على تسجيل الدخول يدويًا في النظام قدر المستطاع وذلك لتجنّب بعض الثغرات الأمنية التي قد تتيح للمخترقين السيطرة على حاسبك. ولا بأس باستخدام تلك الروابط في حال الحرص على نقلها من خلال عناوين بريد إلكتروني خاصة بالجمعية الخيرية أو الجهة غير الربحية آمنة بدلًا من خدمات اجتماعية مشاعة.

٢. تجنب الضغط على روابط لاجتماعات مشبوهة أو من مصادر غير معروفة.



٣. إن لكل غرفة اجتماعات افتراضية «معرّف» يميزها، ويمكن تشبيهه باللوحة التي يتم تثبيتها على أبواب غرف الاجتماعات التقليدية لتمييز كل غرفة عن غيرها. احرص ألّا تشارك معرّف الاجتماع هذا في المنتديات والمنصات الاجتماعية العامة. يفضل الاستعانة في الاجتماعات غير الدورية بمعرفات الاجتماعات العشوائية المؤقتة التي تولدها المنصة لكل اجتماع على حدة.

٤. أقفل غرفتك الافتراضية بحيث لا يمكن الانضمام إليها بعد أن يبدأ الاجتماع.

٥. عند مشاركة أحد نوافذ سطح مكتبك مع مجموعة العمل، تتيح المنصة لأي فرد آخر في الاجتماع أن يطلب منك السيطرة على ما بداخل نافذة حاسبك ليتمكن من التعديل على الوثيقة المشتركة بنفسه. وسيطلب النظام منك قبل ذلك منح الصلاحية التي يطلبها. لا توافق تلقائياً على النوافذ التي تظهر أمامك وتأكّد من محتوياتها وأنّك بالفعل تريد منح تلك الصلاحية، ثم تأكّد من سحب تلك الصلاحية فور انتهاء الحاجة إليها.

٦. على كافة الحضور التعاون لمراقبة قائمة المشاركين والتنبيه فور دخول شخص غير متوقع إلى الجلسة ليتمكن مدير الجلسة من سرعة اتخاذ اللازم، إمّا بالإذن له أو باستبعاده.

٧. من الأفضل لمدير الجلسة في الاجتماعات الكبيرة ألّا يسمح لأي أحد بمشاركة الصوت أو الصورة أو عرض سطح مكتبه دون موافقته.

٨. على مدير الجلسة تذكير كافة الحضور في أول الجلسة بضرورة تجنب مناقشة مواضيع ذات تصنيف (سرّي أو سرّي للغاية) من خلال هذه المنصّات العامة، مع تذكيرهم بأهمية مراعاة أساسيات أمن المعلومات.

٩. عند استخدام منصّات عمل مستضافة خارج الوطن، من الأفضل عدم تحميل ملفات الجمعية الخيرية أو الجهة غير الربحية الحساسة إلى تلك المنصات مهما كانت احتياطاتها الأمنية، والأفضل الاستعاضة عنها بخدمات تخزين الملفات الداخلية المعدّة للموظفين بداخل كل جمعية خيرية أو جهة غير ربحية.

١٠. على الجميع التعاون بعدم الضغط على أي رابط لم يتم إرساله من قبل شخص مصرح، والحذر حتى من الروابط المرسلة من قبل المصرحين، فقد يكون جهاز الشخص المصرح أو حسابه مخترقاً.

١١. عند انتهاء الاجتماع عليك ألّا تنسى أن تضغط على الزر المعد لإنهاء الجلسة لضمان عدم استمرار البث من جانبك دون علمك.

١٢. عند الانتهاء من كافة اجتماعات اليوم، عليك التأكد من إغلاق المنصة بالكامل حفاظًا على خصوصيتك وخصوصية أهل بيتك.

الخطوة السادسة:
أفضل الممارسات لتحصين أنظمة العمل في الجمعيات الخيرية أو الجهات غير الربحية

تذكر دوماً أن تلتزم أيضاً بكافة إرشادات وتقنيات مكان عملك الأمنية وألّا تتجاهلها أو تحاول أن تتخطاها، حيث أنها لم توضع إلّا بعد دراسة متعمقة من المختصين لحمايتك وحماية الجمعية الخيرية أو الجهة غير الربحية ضمن أفضل الممارسات الحديثة مع مراعاة أبرز المخاطر الأمنية المتجددة والتي قد لا تكون على إحاطة بها.

وفيما يلي جملة من التوصيات الأمنية التي من المهم عليك مراعاتها لحماية خصوصيتك الشخصية والعائلية وسرية بيانات عملك عند استخدامك لهذه المنصات:

١. تتيح الجمعيات الخيرية أو الجهات غير الربحية اليوم لمنسوبيها الاستفادة من خدمة «**الشبكات الخاصة الافتراضية VPN**» والتي تنشئ قناة اتصال مشفرة بين حاسبك المنزلي ومركز المعلومات في الجمعية الخيرية أو الجهة غير الربحية ثم تمكنك من الوصول إلى خدماتها المعلوماتية الداخلية من خلالها، مع منع التصنت على تلك القناة والتقاط بياناتك دون علمك. احرص على التواصل مع زملائك منسوبي مكتب الدعم الفني في الجمعية الخيرية أو الجهة غير الربحية للحصول على حساب في تلك الخدمة واتبع التعليمات المعدة لك من قبلهم لخدمتك في تفعيلها.

٢. احرص دوماً على اختيار «جملة سر» بدلاً من كلمة سر لكافة حساباتك الرسمية، مع تضمينها تشكيلة من الحروف والأرقام والرموز .

٣. عند تبادل الملفات بين الموظفين، من الأفضل الاستعانة بخدمات المجلدات المشتركة الداخلية للجمعية الخيرية أو للجهة غير الربحية لضمان السرية وعدم اللجوء إلى الخدمات المشابهة المؤمنة من خلال منصات العمل التعاوني والتنسيق عن بُعد المستضافة خارج الوطن. وفي حال عدم توفر تلك الخدمة بداخل الجمعية الخيرية أو الجهة غير الربحية أو تعذر استخدامها لوجود أعضاء في فريق العمل لا ينتمون إلى نفس الجهة، فاسأل فريق الجمعية الخيرية أو الجهة غير الربحية الأمني عن مدى مناسبة الاستعانة بأنظمة البريد الإلكترونية الرسمي المستضافة داخل الوطن كبديل لتبادلها بين الأعضاء.

٤. تأكّد من أن روابط كافة الصفحات الداخلية للجمعية الخيرية أو للجهة غير الربحية التي تظهر أمامك في المتصفح تبدأ بالنص «**https**» (وبجانبها رمز القفل) بدلاً من النص «**http**» لضمان تشفير كافة عملياتك بداخلها، وبلّغ مكتب الدعم الفني على الفور في حال عدم تحقق ذلك.

٥. تجنّب الضغط على أي روابط تصلك من أي مصدر موثوقًا كان أو غريبًا. وتفحّص الرابط بعناية، وأدخله يدويًا في متصفحك في حال ضرورة تتبعها.

٦. من الأفضل الاستعانة بالتوقيعات الإلكترونية والتشفير الرقمي للمخاطبات الرسمية الحساسة وذلك من خلال الاستفادة من الخدمات المقدمة من قبل المؤسسات الوطنية ذات العلاقة مثل المركز الوطني للتصديق الرقمي، وفي حال عدم توفرها في حاسبك، تواصل مع مكتب الدعم الفني لطلبها.

الخطوة السابعة:
أمن العمل عن بُعد خلال التنقل والسفر

أي تغيير في عادات العمل اليومية من شأنه أن يمثل خطراً أمنياً جديداً محتملاً. ومن نماذج ذلك الخروج من بيئة «المكتب المنزلي» المعد بكافة الاحتياطات الأمنية الواردة في هذه الوثيقة إلى بيئة عمل مؤقتة غير محصّنةً أمنياً، مثل بيئة السفر أو الإقامة في الفنادق أو في منازل الأقارب. عند حدوث ذلك وجب مراعاة ما يلي:

١. تجنّب استخدام الشبكات العامة، كشبكات الفنادق المجانية أو شبكات الجيل الرابع المتنقّلة المملوكة للآخرين، إلى أقصى حد ممكن. حيث يمكن بسهولة استغلالها للتجسس على كافة اتصالاتك ونسخ بياناتك وحساباتك. ومن الأفضل الاستعانة بشبكات شركات الاتصالات التجارية العامة (من نوع **3G** و **4G** و **5G**) عند المقدرة.

٢. احرص دوماً على تفعيل خاصية «**الشبكة الخاصة الافتراضية VPN**» للجمعية الخيرية أو للجهة غير الربحية قبل نقل أي بيانات أو العمل عن بُعد من خلال تلك الشبكات غير الآمنة.

٣. عند التنقل والسفر أو المكوث بداخل المطارات أو الفنادق أو ما شابهها، احذر من شحن أجهزتك الذكية من محطات الشحن المجانية العامة من خلال أسلاك «**يو إس بي**» المعدة لنقل البيانات (الحاوية على أربعة أسلاك داخلية)، ولا تشحنها في تلك الأماكن إلّا من خلال أسلاك «**يو إس بي**» المخصصة للشحن فقط (التي لا تحوي إلّا سلكين داخليين فقط).

٤. احتفظ برقم هاتف مكتب الدعم الفني للجمعية الخيرية أو للجهة غير الربحية معك في كل الأوقات، ولو تمت سرقة جهازك أو انتابك الشك بأنه قد تم اختراقه أو اختراق أحد حساباتك الرسمية، بادر بالتواصل معه فوراً لإيقاف حساباتك واتخاذ التدابير الأمنية المناسبة قبل أن يتم استغلال هويتك أو جهازك لتحميلك تبعات جريمة معلوماتية.

الخطوة الثامنة:
كن واعياً واعرف علامات الخطر

هنالك سمات وظواهر قد تدل على أن جهازك مخترق, من أبرزها:

١. حرارة عالية للجهاز على الدوام حتى وإن كان خاملاً.

٢. بطء غير طبيعي في أداء الجهاز.

٣. نفاذ شحنة البطارية بسرعة.

٤. تصرفات غريبة من حين لآخر في الجهاز مثل حركة في الفأرة أو إضاءة لمبة الكاميرا تلقائياً.

لو حصل أي شيء من ذلك في جهازك سارع بإغلاقه وبالتواصل فوراً مع مكتب الدعم الفني للجمعية الخيرية أو للجهة غير الربحية لفحص جهازك واتخاذ ما يلزم.

تقدّم كافة خدمات العمل عن بُعد الإلكترونية في المملكة العربية السعودية إلى الموظفين **بالمجان**.

لذلك وجب الحذر من أية مراسلات أو تنبيهات آلية تطلب من الموظف دفع مبالغ مالية مقابل الحصول على تلك الخدمات من أطراف مشبوهة أو غير رسمية. ومن المهم التواصل مع مكتب الدعم الفني في الجمعية الخيرية أو الجهة غير الربحية فور حدوث ذلك لإحاطتهم ولتنبيه بقية زملائك، فقد يكون محاولة نصب أو اختراق.

الأنظمة والمؤسسات الرسمية تحميك وتحفظ حقوقك

الجهل لا يعفي الجاني من مسؤولية المتابعة القانونية والجزاءات. وعلى النقيض، فإن الوعي يحفظ حقوق الموظف والمواطن عموما. لذلك من المهم قراءة الأنظمة الوطنية التالية:

١. نظام مكافحة جرائم المعلوماتية.
٢. نظام التعاملات الإلكترونية.
٣. نظام الاتصالات.

ويمكنك الاطلاع عليها جميعاً من خلال زيارة الرابط:

https://www.my.gov.sa/wps/portal/snp/aboutksa/rulesandRegulations

الأنظمة السعودية

واعلم أن راحتك وأمنك من أسمى مقاصد الوطن. وتحقيقاً لذلك فقد أمّن لك العديد من المؤسسات التنظيمية والخدمات الإلكترونية لحفظ حقوقك كموظف وكمواطن أو مقيم ولإرشادك وخدمتك. فاحرص على معرفتها والاستفادة من خدماتها:

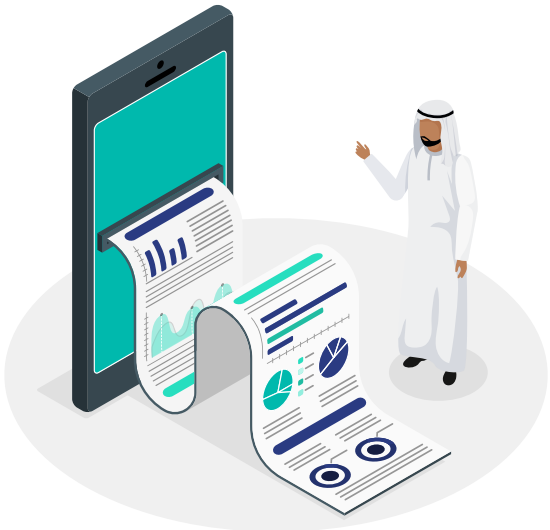
١. للاطلاع على التصنيف الوطني للوثائق الرسمية: المركز الوطني للوثائق والمحفوظات **(ncar.gov.sa)**

٢. للإبلاغ عن جريمة معلوماتية:
تطبيق (كلنا أمن)،
الأمن العام (moi.gov.sa).

٣. عند وجود أسئلة عن أمن المعلومات:
المركز الوطني الإرشادي للأمن السيبراني (cert.gov.sa).

٤. للمشاكل في خدمات الاتصالات:
هيئة الاتصالات وتقنية المعلومات (www.citc.gov.sa)

٥. للإبلاغ عن محتوى معلوماتي سلبي:
موقع إنترنت السعودية (internet.sa)،
اللجنة الوطنية لتقنين المحتوى الأخلاقي لتقنية المعلومات (ncdcr.gov.sa)




الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority