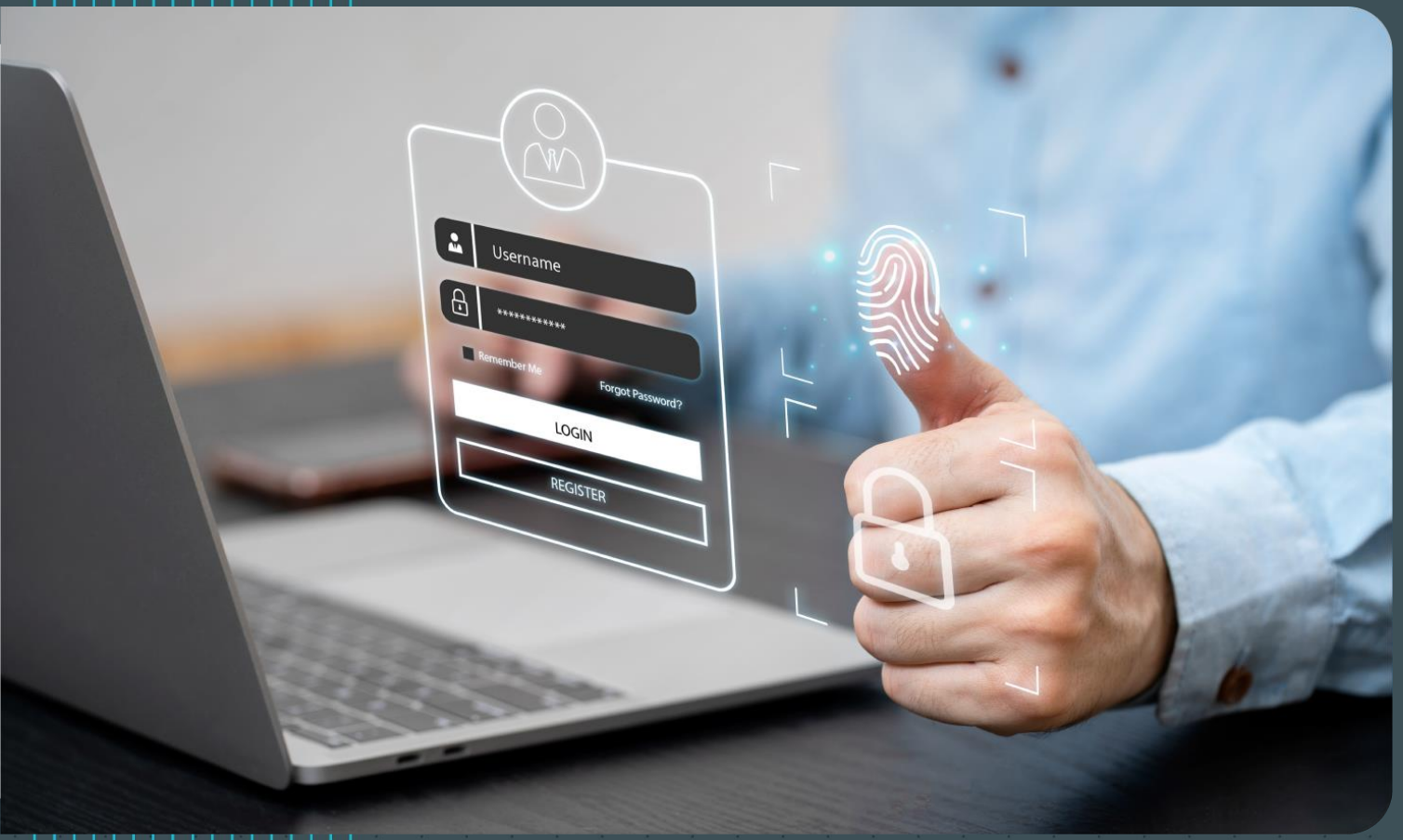
المركز الوطني
للأمن السيبراني
National Cyber
Security Center



مسؤوليات المُستخدمين والصلاحيات

المحـــــاور

- مقدمة عن مسؤوليات المُستخدمين والصلاحيات
- تعريف مسؤوليات المُستخدِمين
- المسؤوليات التي يتوجب على المُستخدِمين الالتزام بها
- تعريف صلاحيات الوصول
- ضوابط تعيين صلاحيات الوصول
- الخاتمة

مقدمة عن مسؤوليات المُستخدمين والصلاحيات

يُعتبر موضوع مسؤوليات المُستخدِمين وتحديد صلاحياتهم في الوصول للأنظمة والمعلومات أمراً بالغ الأهمية في تحقيق الأمن السيبراني لأي مؤسسة أو دائرة وعنصراً هاماً في سياق استخدام التكنولوجيا والأنظمة المعلوماتية؛ ففهم المُستخدِمين لمسؤولياتهم وتنظيم الصلاحيات يُسهم وبشكل كبير في تحقيق أمان وفعالية أفضل للأنظمة والبيانات، وسنتعرف في الآتي بشكل أكبر عن كل من مفهوم مسؤوليات المُستخدِمين ومفهوم صلاحيات الوصول.

تعريف مسؤوليات المُستخدِمين

- يُقصد بمسؤوليات المُستخدمين الواجبات والالتزامات التي يتحملها الموظفين أو الأفراد عند استخدام أنظمة تكنولوجيا المعلومات المختلفة سواء الداخلية الخاصة بالمؤسسة أو الخارجية المربوطة على شبكة الإنترنت.

- يُعنى هذا المفهوم باتخاذ التدابير وإتباع الإجراءات اللازمة التي تضمن للمُستخدِم حماية معلوماته الشخصية والمعلومات والبيانات الحساسة ضمن مؤسسته، وبما لا يعرض سلامة الأنظمة الرقمية والأجهزة للخطر أو التهديد السيبراني.

المسؤوليات التي يتوجب على المُستخدِمين الالتزام بها

يوضح الآتي بعض من المسؤوليات التي يتوجب على المُستخدِمين الالتزام بها لضمان أمنهم السيبراني وحمايتهم الرقمية:

الحفاظ على كلمات المرور:

- يجب أن يختار المُستخدِم كلمة مرور قوية ومُركبة بحيث تتضمن مزيجاً من الأحرف الكبيرة والصغيرة والأرقام والرموز.
- يجب أن تكون عشوائية بحيث لا يُمكن توقعها أو التنبؤ بها.
- يقع على المُستخدِم مسؤولية حماية كلمة المرور الخاصة به من خلال عدم مُشاركتها مع الآخرين وتجنُب كتباتها على مكان ظاهر للآخرين، وغيرها من الإجراءات التي تضمن عدم معرفتها أو الاطلاع عليها.

المسؤوليات التي يتوجب على المُستخدِمين الالتزام بها

تلافي تهديدات الهندسة الاجتماعية:

- يجب على كل مُستخدِم التصدي لهجمات الهندسة الاجتماعية المختلفة من خلال التحقُّق من هوية مصداقية المُرسلِين وعدم مُشاركة المعلومات الحساسة أو حتى الشخصية عبر وسائل ومواقع التواصل الاجتماعي لتجنُّب استغلالها من قبل المُتصيدين لشن هجماتهم بالاعتماد على تلك المعلومات.

المسؤوليات التي يتوجب على المُستخدِمين الالتزام بها

إدارة البريد الإلكتروني بعناية:

- في قوانين أمن المعلومات والأمن السيبراني فإن كل مُستخدِم مسؤول عن حماية بريده الإلكتروني، لذا فإنه يتوجب التحقق من أي مرفقات أو روابط غريبة يتم استقبالها عبر البريد الإلكتروني سواء الشخصي أو حتى الرسمي.
- ينبغي الابتعاد عن الرد على أي رسائل غريبة وغامضة والتفاعل معها وخاصة تلك التي يتم فيها مُطالبة المُستخدِم بإجراء فوري كتغيير كلمة المرور، حيث عادة ما تكون تلك الرسائل هجمات تصيد احتيالي تهدف إلى خداع المُستخدِم واختراق بياناته والتجسس عليها.

المسؤوليات التي يتوجب على المُستخدِمين الالتزام بها

الحفاظ على الأجهزة:

- من المسؤوليات الهامة التي يتوجب على المُستخدِمين الحرص على تطبيقها حماية الأجهزة ومنع تعرضها للسرقة أو الفقد حيث يؤدي هذا الأمر إلى الوصول إلى المعلومات الموجودة على الجهاز والاطلاع عليها وهو ما قد يُعرض المُستخدِم للمساءلة القانونية.

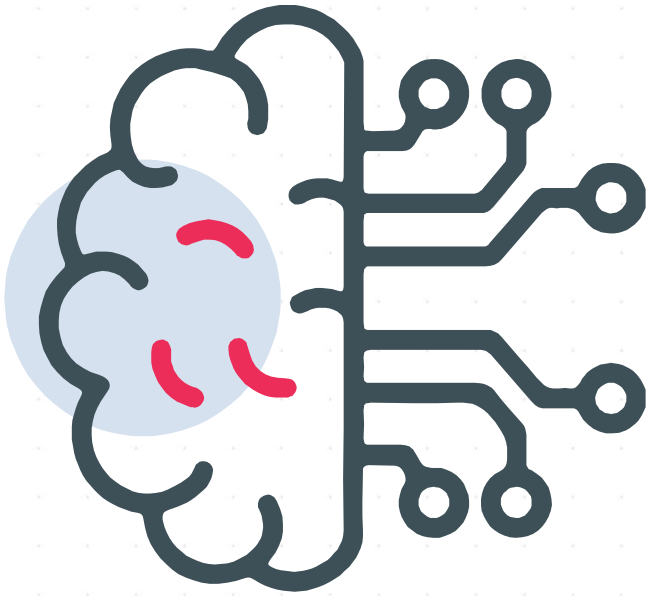
- من الإجراءات الهامة في مجال الحفاظ على الأجهزة تأمينها وحمايتها رقمياً من خلال كلمات المرور المُعقدة وتفعيل أنظمة التحقق الثنائي خلالها.

المسؤوليات التي يتوجب على المُستخدِمين الالتزام بها

الالتزام بالسياسات الأمنية:

- على كل مُستخدِم التحقق من أنه يلتزم بالسياسات الأمنية الصادرة عن مؤسسته وتطبيق قواعد الأمان التي يفرضها قسم تكنولوجيا المعلومات أو قسم الأمن السيبراني.

المسؤوليات التي يتوجب على المُستخدِمين الالتزام بها



التطوُر والتعلُم:

- من الجدير بالذكر أن جهل المُستخدِم بإجراءات وتدابير الأمن السيبراني التي يتوجب تطبيقها لا تعفيه من المساءلة القانونية التي قد تطاله في حالة وقوع حادث أو هجمة سيبرانية تم شنها على المؤسسة من خلاله.

- يجب على المُستخدِم أن يقوم بتوعية نفسه أو يقوم بطلب المُساعدة من خبراء تكنولوجيا المعلومات حيال كيفية تحقيق الأمن السيبراني وتجنُب الوقوع كضحية للتهديدات والهجمات الرقمية المختلفة.

المسؤوليات التي يتوجب على المُستخدِمين الالتزام بها

الإبلاغ عن الحوادث السيبرانية:

- في حال اشتباه المُستخدِم بأنه تم اختراق جهازه أو نظامه في المؤسسة فإنه يتوجب أن يقوم بالتبليغ عن ذلك لرؤسائه ولمختصي الأمن السيبراني وتكنولوجيا المعلومات في مؤسسته.

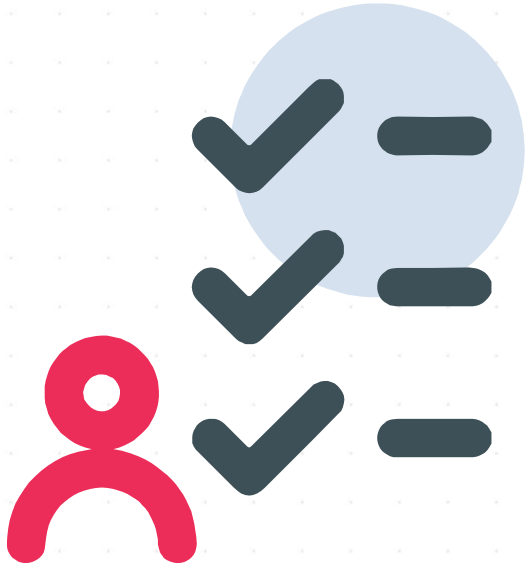
- إذا تعرّضت بالمركز الوطني للأمن السيبراني للاختراق أو للتهديد، أو انتحال للشخصية، أو وصلك بريد منتحل لجهة رسمية وطنية أو وردك اتصال من شخص منتحل.. ساهم بالإبلاغ من خلال:

✓ الإرسال إلى البريد الإلكتروني:
✓ الاتصال على رقم التواصل:
✓ التواصل مع إدارة الأمن في:

تعريف صلاحيات الوصول

يُقصد بصلاحيات الوصول تحديد مجموعة من الإمكانيات والصلاحيات والامتيازات التي يتم منحها للمُستخدِمين تبعاً لدورهم في المؤسسة وما يتطلبه موقعهم الوظيفي، بحيث يكون كل مُستخدِم قادراً على الوصول إلى المعلومات والبيانات التي تُمكنه من إجراء المهام المطلوبة منه في نطاق العمل دون أن يكون قادراً على الاطلاع أو الوصول إلى بيانات وأنظمة لا تتوافق مع منصبه الوظيفي ومتطلبات عمله، ومن شأن هذا المفهوم تحديد مدى قدرة المُستخدِمين على الوصول إلى المعلومات والموارد الخاصة بالمؤسسة.

ضوابط تعيين صلاحيات الوصول



يوجد العديد من الضوابط التي يتوجب مراعاتها عند وضع صلاحيات المُستخدِمين وتحديد مدى ما يُمكن منحه لكل منهم من صلاحيات وإمكانيات للوصول إلى المعلومات والأنظمة، ومن أبرز هذه الضوابط:

ضوابط تعيين صلاحيات الوصول

مبدأ أقل صلاحية:

- إن وضع صلاحيات وصول المُستخدِمين للموارد والأنظمة في المؤسسة يجب أن يتم وفق مبدأ حاجتهم للوصول فقط إلى المعلومات والبيانات التي تُمكنهم من أداء مهامهم على أتم وجه.

تحديد الصلاحيات:

- يجب تقسيم الصلاحيات التي يتم منحها للمُستخدِمين إلى مستويات دقيقة بحيث يتم تحديد صلاحيات مُعينة لمهام مُعينة.

- مسؤولي الحسابات المالية لا يتوجب أن يكون لديهم صلاحية تثبيت البرامج وإضافتها على سبيل المثال لا الحصر.

ضوابط تعيين صلاحيات الوصول

المراجعة المُستمرة:

- ينبغي أن تخضع عملية منح الصلاحيات للمُستخدمين إلى المراجعة المُستمرة من قبل مختصي تكنولوجيا المعلومات في المؤسسة.
- يكون ذلك لضمان أن هذه الصلاحيات لا تزال ملائمة لاحتياجات المُستخدِم دون نقص أو زيادة في إمكانية الوصول وبما يُمكنه من أداء مهامه.

ضوابط تعيين صلاحيات الوصول

تفعيل سجلات الوصول:

- وهي أدوات تقنية تُمكن مسؤولي الأنظمة من متابعة وتسجيل جميع الأنشطة المتعلقة بوصول المُستخدِمين إلى الحسابات والأجهزة المُختلفة، وهو ما يُتيح رصد استخدام صلاحيات كل مُستخدِم والكشف عن أي حركة أو نشاط غير طبيعي ومشبوه.

الخاتمة

أن فهم المُستخدِمين لمسؤولياتهم وكذلك تحديد صلاحيات وصولهم للموارد المختلفة كالحسابات والاجهزة يُسهم وبشكل كبير في تحقيق الأمن السيبراني للمؤسسة والمنظومة بشكل كامل، ويحمي المُستخدِم نفسه من التهديدات السيبرانية المختلفة.

نتمنى لكم السلامة في

العالم

الرقمي.