الدليل الإرشادي للأمن الرقمي (خطوات عملية للموظفين)

هذا الدليل هو "خارطة الطريق" اليومية للموظف لضمان حماية بيئة العمل

المقدمة وأهمية دور الموظف

مع تزايد الاعتماد اليومي على التكنولوجيا في تسيير المعاملات، لم يعد الأمن السيبراني ترفاً تقنياً، بل أصبح ضرورة ملحة لجميع الشركات في ليبيا مهما كان حجمها، سواء كانت مؤسسات كبرى أو مشروعات متناهية الصغر وصغرى ومتوسطة. يهدف هذا الدليل إلى تبسيط مفاهيم الأمن الرقمي وتقديم إرشادات عملية وبسيطة تساعد الموظفين وفرق العمل على حماية أنظمتهم وبياناتهم من الهجمات السيبرانية المتزايدة.

إن الهدف الأساسي من هذه الإرشادات هو تعزيز "ثقافة الأمن السيبراني" والوعي المجتمعي داخل بيئة العمل، انطلاقاً من مبدأ أن الموظف المدرب والواعي هو خط الدفاع الأول والأساسي ضد أي اختراق. من خلال تطبيق هذه الخطوات، نهدف إلى تعزيز ثقة العملاء والشركاء، وضمان بقاء بيئة العمل الرقمية آمنة ومستقرة، مما يقلل من المخاطر ويحمي سمعة المؤسسة في السوق الليبي

المبادئ العملية للأمن الرقمي

- **الوقاية الذاتية:** الحذر الدائم والشك الإيجابي في التعامل مع الطلبات الرقمية غير المعتادة.
- **الشفافية والإبلاغ:** الصدق والسرعة في التبليغ عن أي خطأ أو اختراق محتمل يقلل من حجم الضرر بنسبة كبيرة.
- **السرية المهنية:** بيانات المؤسسة والعملاء أمانة لا يجوز تداولها عبر القنوات غير الرسمية (مثل تطبيقات الدردشة الشخصية).

إرشادات العمل اليومي (تفصيلية)

- **إدارة الحسابات:** يجب استخدام كلمات مرور قوية (تجمع بين الحروف، الأرقام، والرموز) مع تفعيل خاصية "التحقق الثنائي" (FA2) أينما توفرت. يُمنع منعاً باتاً مشاركة كلمات المرور مع الزملاء أو كتابتها في أماكن مكشوفة.
- **أمن البريد الإلكتروني:** احذر من رسائل "الهندسة الاجتماعية" التي تطلب منك النقر على روابط مشبوهة أو تحميل ملفات مجهولة. تأكد دائماً من هوية المرسل، وفي حال الشك، تواصل معه عبر وسيلة اتصال أخرى للتحقق.
- **حماية الأجهزة المحمولة:** عند استخدام الهواتف أو الحواسيب المحمولة الخاصة بالعمل، يجب التأكد من قفل الشاشة عند مغادرة المكتب، وتجنب استخدام شبكات "الواي فاي" العامة والمفتوحة للوصول إلى أنظمة الشركة.

بروتوكول الاستجابة للحوادث (ماذا تفعل عند وقوع الخطر؟)

إذا اشتبهت في وجود اختراق (مثل بطء مفاجئ، ظهور نوافذ غريبة، أو فقدان ملفات)، اتبع الخطوات التالية فوراً:

1. **عزل الجهاز:** افصل كابل الإنترنت أو أغلق الواي فاي لمنع المتسلل من سحب البيانات أو الانتشار لأجهزة أخرى.
2. **التواصل الفوري:** أبلغ مسؤول الأمن الرقمي أو مديرك المباشر فوراً دون محاولة إخفاء الأمر.
3. **تأمين الحسابات:** قم بتغيير كلمات المرور الخاصة بك من جهاز آخر سليم، وراقب أي نشاط غير مصرح به في بريدك الإلكتروني.
4. **التعاون التقني:** قدم كافة التفاصيل للفريق الفني لمساعدتهم في استعادة البيانات من النسخ الاحتياطية وتحديد مصدر الاختراق.

خاتمة

إن أمننا الرقمي يبدأ من "نقرة" واعية وتنتهي ببيئة عمل محمية. شكراً لالتزامكم بكونكم الحارس الأول لنجاح واستمرارية هذه المؤسسة.