دليل الأمن السيبراني

برنامج التوعية بالأمن السيبراني

حماية بياناتك مسؤولية الجميع

دليل إرشادي مختصر وفق هوية منصة «توعية» - مقاس A5

tawiyah.sa | 2026

المحتويات

نظرة سريعة على الدليل

المقدمة

الأمن السيبراني يبدأ من المستخدم

	**لماذا هذا الدليل؟** في عالم رقمي متسارع، أصبح الأمن السيبراني مسؤولية فردية قبل أن يكون مسؤولية مؤسسية. يهدف هذا الدليل إلى تزويدك بالمعرفة الأساسية لحماية نفسك وبيانات مؤسستك من التهديدات الإلكترونية.

ماذا ستتعلم؟

- ✓ إنشاء كلمات مرور قوية وإدارتها.
- ✓ اكتشاف رسائل التصيد الاحتيالي.
- ✓ فهم أهمية التحديثات الأمنية.
- ✓ اتباع ممارسات آمنة عند العمل عن بعد.
- ✓ التعامل الآمن مع البريد الإلكتروني.

كلمات المرور الذكية

قاعدة بسيطة لحماية حساباتك

	قاعدة 3-1-2 استخدم 3 أحرف كبيرة، ورمزًا خاصًا واحدًا مثل @ أو # أو !، ورقمين على الأقل. مثال توضيحي: Salam@Amn26

ممارسات مهمة

- ✓ لا تستخدم كلمة المرور نفسها في أكثر من موقع.
- ✓ غيّر كلمة المرور بشكل دوري عند الحاجة أو عند الاشتباه.
- ✓ استخدم مدير كلمات مرور موثوق.
- ✓ تجنب استخدام اسمك أو تاريخ ميلادك أو رقم جوالك.
- ✓ فعّل المصادقة متعددة العوامل متى ما كانت متاحة.

التصيد الاحتيالي

كيف تكتشف الرسائل المشبوهة؟

العلامة	ما الذي تنتبه له؟
مرسل غير معروف	تحقق من عنوان البريد بالكامل قبل الرد أو النقر.
لغة عاجلة	عبارات مثل: تحرك الآن، حسابك سيغلق، فرصة أخيرة.
روابط مشبوهة	مرر المؤشر فوق الرابط وتأكد من النطاق الحقيقي.
مرفقات غير متوقعة	لا تفتح المرفقات قبل التأكد من مصدرها.
أخطاء إملائية	قد تكون علامة على رسالة احتيالية أو انتحال.

قاعدة التعامل مع التصيد

توقف، تحقق، أبلغ

!	قاعدة ذهبية إذا كنت في شك، لا تنقر. تواصل مع فريق الأمن السيبراني فورًا قبل اتخاذ أي إجراء.

خطوات التعامل مع رسالة مشبوهة

✓ توقف ولا تستعجل بالرد أو النقر.

✓ تحقق من المرسل والرابط والمرفقات.

✓ أبلغ الفريق المختص وأرفق لقطة شاشة عند الحاجة.

التحديثات الأمنية

تحديثات اليوم تحمي بيانات الغد

لماذا التحديثات مهمة؟ تغلق التحديثات الثغرات المعروفة وتحسن حماية الأجهزة والتطبيقات. تأجيل التحديثات قد يترك الجهاز مكشوفًا أمام مخاطر يمكن تجنبها.	

ممارسات أساسية

- ✓ فعّل التحديثات التلقائية.
- ✓ لا تؤجل تحديثات النظام الحرجة.
- ✓ حدّث متصفح الإنترنت باستمرار.
- ✓ حدّث تطبيقات الهاتف بانتظام.
- ✓ أعد تشغيل الجهاز بعد التحديث إذا طُلب ذلك.

أمن العمل عن بعد

اتصال آمن من أي مكان

- ✓ استخدم شبكة VPN للاتصال بالشبكة الداخلية.
- ✓ تأكد من تحديث جهاز التوجيه واستخدام كلمة مرور قوية.
- ✓ لا تترك الشاشة مفتوحة في الأماكن العامة.
- ✓ استخدم قفل الشاشة عند الابتعاد عن الجهاز.
- ✓ افصل الأجهزة غير المستخدمة عن الشبكة.
- ✓ استخدم سماعة رأس للاجتماعات الحساسة.
- ✓ تأكد من خصوصية المكان أثناء الاجتماعات.

⌂	تذكير سريع الأمان في العمل عن بعد لا يعتمد على التقنية فقط؛ بل يعتمد على وعي المستخدم وسلوكه اليومي.

البريد الإلكتروني الآمن

افتح بوعي، وارسل بمسؤولية

✓ تحقق من العنوان الكامل للمرسل قبل مشاركة أي بيانات.

✓ لا ترسل كلمات مرور أو رموز تحقق عبر البريد.

✓ استخدم عناوين واضحة وتجنب الملفات غير الضرورية.

✓ افحص الروابط قبل النقر عليها.

✓ لا تحمل المرفقات من مصادر غير معروفة.

✓ أبلغ عن أي رسالة مشبوهة فورًا.

@	قاعدة التعامل البريد الإلكتروني هو أكثر قنوات الهجمات شيوعًا؛ كل رسالة غير متوقعة يجب أن تعامل بحذر حتى يثبت العكس.

نقاطك السريعة

خمس ممارسات لا تتنازل عنها

#	الممارسة
1	استخدم كلمة مرور فريدة وقوية لكل حساب.
2	فعّل المصادقة متعددة العوامل دائمًا.
3	اشتبه في كل بريد إلكتروني غير متوقع.
4	حدّث أجهزتك فور صدور التحديثات.
5	أبلغ فريق الأمن عن أي نشاط مشبوه.

✓

الأمن السيبراني يبدأ منك

قرار بسيط مثل التحقق قبل النقر يمكن أن يمنع حادثًا أمنيًا كاملًا.

جهات الاتصال والبلاغات

عند الشك أو الطوارئ

القناة	التفاصيل
فريق الاستجابة للحوادث السيبرانية	security@company.com
رقم التواصل	800-123-4567 | داخلي: 5555
التوفر	متاح 24/7
الإبلاغ عن التصيد	phishing@company.com
تطبيق البلاغات الداخلي	CyberSafe

قبل البلاغ

احتفظ بصورة من الرسالة أو الرابط أو الشاشة، ولا تحذف الدليل قبل إبلاغ الفريق المختص.

المراجع ومعلومات الإصدار

هوية موحدة قابلة لإعادة الاستخدام

§

المرجع الأساسي

تم إعداد هذا الدليل اعتمادًا على المستند المرفق: «دليل الأمن السيبراني - برنامج التوعية بالأمن السيبراني»، مع إعادة تنظيم المحتوى بصيغة A5 وفق هوية شعار منصة «توعية».

البند	القيمة
اسم البرنامج	برنامج التوعية بالأمن السيبراني
اسم المنصة	توعية | Tawiyah
رابط الموقع	https://tawiyah.sa
الإصدار	2026
ملاحظة	يمكن تعديل البريد والأرقام والروابط حسب الجهة.

شكرًا لالتزامك بأمن المؤسسة. معًا نبني بيئة رقمية آمنة.