KFU
جامعة الملك فيصل
KING FAISAL UNIVERSITY
جـامعة ووطـن..نمـاء..واسـتدامة..

# دليل الممارسات السيبرانية الآمنة في بيئة عمل جامعة الملك فيصل

# المحتويات

## مقدمة

تشهد المملكة تحولاً واسع النطاق في استخدام أنظمة تقنية المعلومات سواءً في مقر العمل أو عن طريق الخدمات المقدمة عن بُعد، مما قد يصاحب ذلك التعرض إلى الهجمات السيبرانية والاختراقات الأمنية، بالإضافة إلى تهديداتٍ مختلفةٍ في تسريب البيانات الحساسة، وانتهاكات لخصوصية الأفراد والجهات. ولرفع موثوقية وانسيابية المعلومات وأمانها وتكامل أنظمتها، فقد تم بناء الاستراتيجية الوطنية للأمن السيبراني التي تعكس الطموح الاستراتيجي للمملكة وبأسلوب متوازن بين الأمان والثقة والنمو . ولضمان تحقيق الأمن السيبراني في أي جهة، لا بد من تحقيق ثلاثة عناصر رئيسية هي: العنصر التقني، العنصر الإجرائي، والعنصر البشري.

قامت جامعة الملك فيصل بإعداد دليل الممارسات السيبرانية الآمنة للموظفين في بيئة عمل الجامعة بناءً على دليل الممارسات السيبرانية الآمنة والذي تم إصداره من قِبل المركز الوطني الإرشادي للأمن السيبراني والهيئة الوطنية للأمن السيبراني والذي يتمحور حول محور ممارسات العنصر البشري وتأثيرها على الأمن السيبراني في الجهات. حيث تفيد إحصاءات الأمن السيبراني بأن ما يقارب 50٪ من الاختراقات التي تشهدها الجهات عالميًا هي بسبب الموظفين بصفة عامة سواءً كانوا موظفين إداريين أو تقنيين أو مدراء تنفيذيين أو حتى اختصاصيين في الأمن السيبراني(*). ومن هذا المنطلق فقد تم إعداد هذا الدليل ليستهدف جميع منسوبي الجامعة على اختلاف أدوارهم بهدف نشر الوعي بالأمن السيبراني ودعم جهودهم نحو رفع الحس الأمنية وحماية جهاتهم وبيناتهم من الهجمات والاختراقات والتهديدات السيبرانية.

## أبرز أسباب التهديدات والاختراقات السيبرانية في بيئة العمل والمرتبطة بالعنصر البشري هي:


(*) دليل الممارسات السيبرانية للموظفين في بيئة العمل

## الفصل الأول:

### التعامل الآمن مع خدمات البريد الإلكتروني ورسائل التصيد الإلكتروني:

- الحذر من الرسائل التي تطلب تحديث البيانات.
- التأكد من صحة البريد الالكتروني.
- عدم الرد على أي رسائل مجهولة المصدر من خلال البريد الالكتروني.
- التأكد من محتوى الرسالة وعدم الضغط على أي رابط إلا بعد التحقق منه.
- تجنب استخدام بريد العمل للأغراض الشخصية.
- عدم كتابة بريد العمل في نماذج التسجيل الإلكترونية (Registration Form) أو مواقع وسائل لتواصل الاجتماعي تفاديًا لتسريبه والاستفادة منه في التخطيط للاختراق.

## الفصل الثاني:

### التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين:

- قم بتحديث نظام التشغيل ومتصفح الانترنت بصفة دورية ومباشرة من مصدر موثوق.
- قم بإزالة ملفات التخزين المؤقتة cookies بصفة دورية.
- لا تستخدم وسائط التخزين الخارجية.
- استخدم كلمة مرور معقدة.
- لا تقم بتوصيل أي وسائط تخزين غير آمنة أو غير معروفة بجهازك بغرض نقل وتبادل الملفات.
- تأكد من أن برنامج جدار الحماية مفعلا على جهازك.
- تأكد دائما من فحص وسائط التخزين الشخصية ببرامج معتمدة للكشف عن البرمجيات الضارة قبل قراءة البيانات منها.
- تجنب تثبيت البرامج المقرصنة أو المجانية على أجهزة جهة العمل أو أجهزتك الشخصية.

**الهندسة الاجتماعية:** الاحتيال على المستخدمين، وإخداعهم للكشف عن معلومات حساسة وخاصة بهدف استغلالها الحقاً لتنفيذ الهجوم على الأفراد والجهات.

**التصيّد الإلكتروني:** أن يقوم المهاجمين بإيهام المستخدمين بمعرفة معلومات كافية عنهم للاستجابة لمتطلباتهم إما للحصول على معلومات حساسة أو تحويل الأموال لهم وغيرها.

## الفصل الثالث:

### التعامل الآمن مع خدمات تصفح الإنترنت:

- لا تستخدم خاصية الدخول التلقائي.
- احرص على مسح المحفوظات والملفات المؤقتة من المتصفح بشكل مستمر.
- استخدم أحدث إصدار من برنامج متصفح الانترنت.
- امنع النوافذ المنبثقة، فبعضها ربما يشكل هجمات خبيثة أو خفية.
- تأكد من ضبط إعدادات الأمان والخصوصية لمتصفح الإنترنت.
- تأكد من تصفح المواقع التي تحتوي على البروتكول الآمن HTTPS.

## الفصل الرابع:

### التعامل الآمن مع وسائل التواصل الاجتماعي:

- تجنّب استخدام وسائل التواصل الاجتماعي عند تبادل البيانات أو الوثائق الخاصة بالعمل.
- لا تقم بنشر المعلومات الحساسة أو الشخصية أو الوظيفية عبر مواقع التواصل الاجتماعي او الانترنت.
- لا تستخدم خاصية تسجيل الدخول التلقائي .
- احرص على تعطيل الموقع الجغرافي للأجهزة وعمل إقفال (Lockout) للأجهزة .
- الحرص على تفعيل وتحديث الأسئلة الأمنية وتوثيقها في مكان آمن.
- استخدام التحقق من الهوية متعدد العناصر .(Multi-Factor Authentication)
- الحرص على تثبيت التحديثات والإصلاحات الأمنية لتطبيقات التواصل الاجتماعي.
- تجنب تسجيل الدخول باستخدام أجهزة أو شبكات عامة غير موثوقة.

**HTTPS:**

(بروتوكول نقل الروابط النصية الآمن): هو بروتوكول لاتصالات الإنترنت يحمي صحّة وسرية بيانات المستخدم أثناء نقلها بين جهاز الحاسب الخاص به وموقعه الإلكتروني.

KFU
جامعة الملك فيصل
KING FAISAL UNIVERSITY
جـامعة ووطـن .. نمـاء .. واسـتدامة ..