جامعة الملك سعود
King Saud University
الإدارة العامة للأمن السيبراني

دليل استخدام
الإبلاغ عن حادثة سيبرانية

جدول التعريفات:

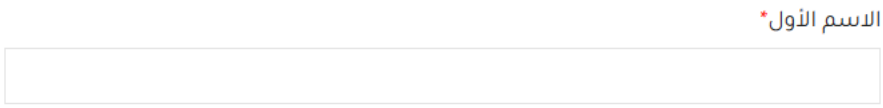
المصطلح	التعريف
التأثير	حجم الضرر أو النتيجة المترتبة على حدوث الثغرة أو الهجوم الأمني، مثل تعطيل الخدمة أو فقدان البيانات.
الحادثة	أي حدث أمني غير مرغوب فيه أو مريب قد يؤثر على سرية أو سلامة أو توفر المعلومات.
رسائل تصيد	رسائل احتيالية تُرسل غالبًا عبر البريد الإلكتروني أو وسائل التواصل بهدف خداع المستخدم للحصول على معلومات حساسة أو تثبيت برمجيات خبيثة.
اختراق	الوصول غير المصرح به إلى نظام أو بيانات أو شبكة بهدف التعديل أو السرقة أو التخريب.
IP	عنوان بروتوكول الإنترنت، وهو رقم فريد يُستخدم للتعريف بجهاز أو خادم على الشبكة.
نظام التشغيل	البرنامج الأساسي الذي يدير أجهزة الحاسوب أو الهواتف ويمكّن تشغيل التطبيقات، مثل Windows أو Linux أو Android.
الشبكة	مجموعة من الأجهزة المترابطة التي تتواصل مع بعضها لتبادل البيانات، مثل شبكة الإنترنت أو الشبكات المحلية.
تسريب البيانات	الكشف غير المصرح به عن معلومات حساسة أو سرية، سواء عن طريق الخطأ أو نتيجة هجوم إلكتروني.
موقع	صفحة أو مجموعة صفحات على الإنترنت يمكن الوصول إليها عبر متصفح باستخدام عنوان URL محدد.
ثغرة	خلل أو نقطة ضعف في النظام أو التطبيق يمكن استغلالها لتنفيذ هجوم أو الوصول غير المصرح به.
برامج الفدية	نوع من البرمجيات الخبيثة يقوم بتشفير ملفات الضحية ويطلب فدية مالية مقابل فك التشفير.

أهداف الدليل:

يهدف هذا الدليل إلى مساعدة المستخدمين على فهم آلية استخدام خدمة الإبلاغ عن حادثة سيبرانية بشكل صحيح وفعال، من خلال شرح خطوات الإبلاغ وتوضيح المصطلحات الفنية المرتبطة. يضمن الدليل سهولة الوصول إلى المعلومات وسرعة التعامل مع أي بلاغ أمني. كما يساهم في تعزيز الوعي الأمني ورفع جودة الخدمة المقدمة.

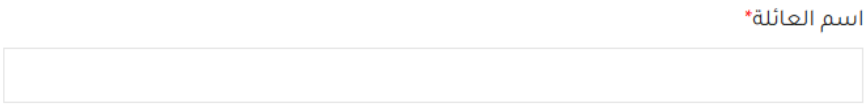
دليل الاستخدام:

1- الاسم الأول:



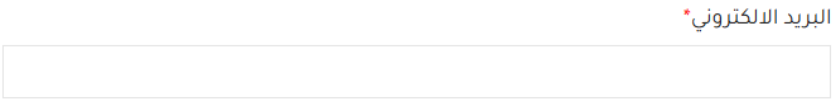
يتم كتابة الاسم الاول للشخص مرسل البلاغ لسهولة التواصل والمتابعة إن لزم.

2- اسم العائلة:



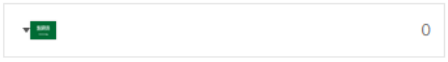
يتم كتابة اسم عائلة الشخص مرسل البلاغ لسهولة التواصل والمتابعة إن لزم.

3- البريد الالكتروني:



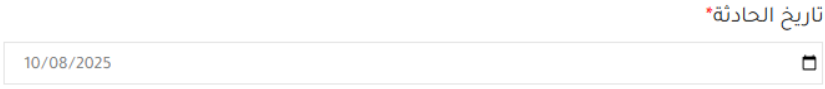
يتم كتابة البريد الالكتروني للشخص مرسل البلاغ لسهولة التواصل والمتابعة إن لزم.

4- رقم الجوال:



يتم كتابة رقم الجوال للشخص مرسل البلاغ لسهولة التواصل والمتابعة إن لزم.

5- تاريخ الحادثة:

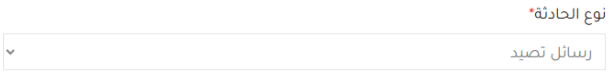


يتم تحديد تاريخ اليوم الذي تمت فيه الحادثة أو ملاحظتها.

6- نوع الحادثة:

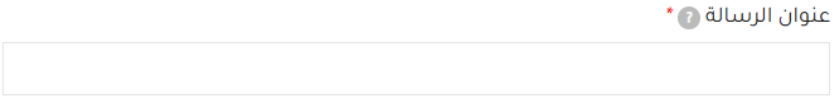
يتم اختيار نوع الحادثة التي تمت على أنظمة الجامعة أو بياناتها أو خدماتها.

أ. رسائل التصيد:



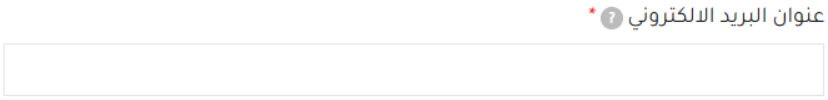
رسائل تصيد

- عنوان الرسالة:



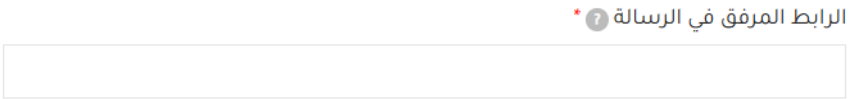
يتم كتابة عنوان رسالة التصيد الظاهر في البريد الالكتروني المستلم.

- عنوان البريد الالكتروني:



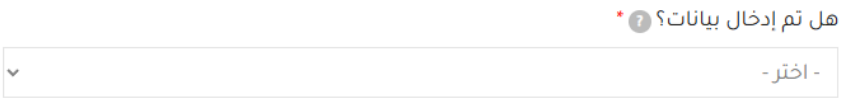
يتم كتابة عنوان البريد الالكتروني للمرسل كما هو ظاهر في رسالة التصيد.

- الرابط المرفق في الرسالة:



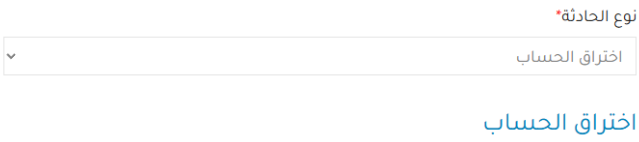
يتم لصق الرابط المرفق في رسالة التصيد مع مراعاة عدم زيارة الرابط.

- هل تم إدخال بيانات؟

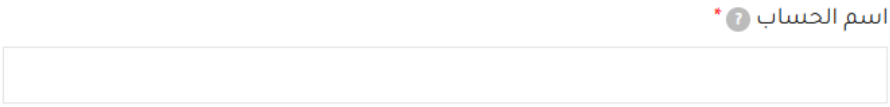


يتم الجواب بنعم أو لا عن هل تم إدخال بيانات في الرابط المرفق في رسالة التصيد أم لا.

ب. اختراق الحساب:

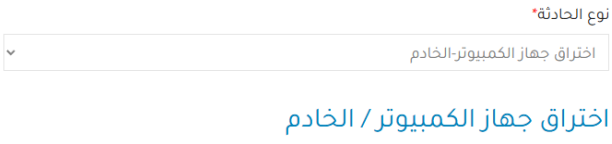


- اسم الحساب:

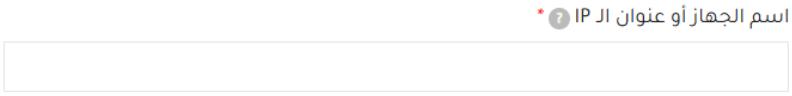


يتم كتابة اسم الحساب أو البريد الالكتروني الذي تم اختراقه.

ج. اختراق جهاز الكمبيوتر – الخادم:

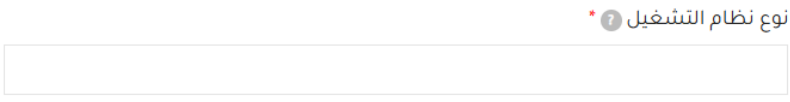


- اسم الجهاز أو عنوان الـ IP:



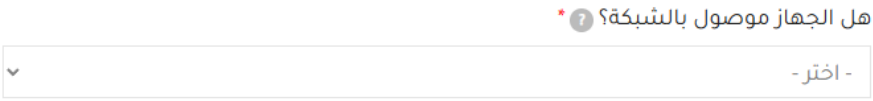
يتم كتابة اسم الجهاز أو عنوان الـ IP الخاص بالجهاز أو الخادم الذي تعرض للاختراق.

- نوع نظام التشغيل:



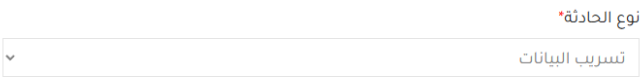
تحديد نوع نظام التشغيل المستخدم في الجهاز أو الخادم المستهدف، مع ذكر الإصدار.

- هل الجهاز موصول بالشبكة؟



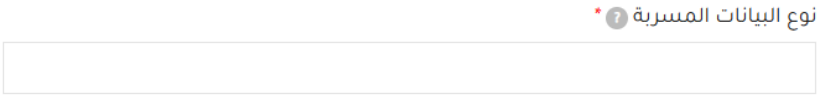
تحديد ما إذا كان الجهاز أو الخادم لا يزال متصلاً بالشبكة حالياً أم تم فصله أو إيقاف تشغيله بعد الحادثة كإجراء وقائي.

د. تسريب البيانات:



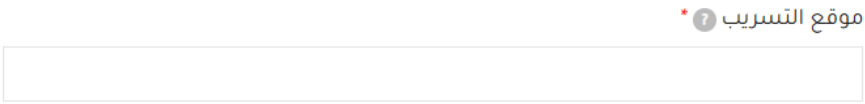
تسريب البيانات

- نوع البيانات المسربة:



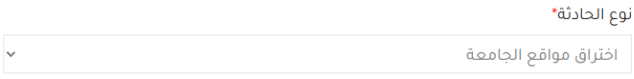
تحديد نوع البيانات التي تم تسريبها مثل بيانات شخصية أو مالية أو معلومات حساسة أخرى.

- موقع التسريب:



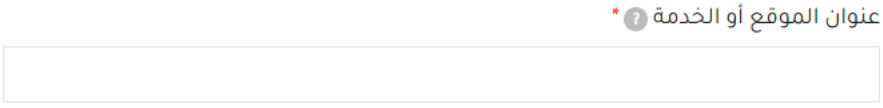
ذكر الموقع أو النظام الذي حدث فيه تسريب البيانات مثل موقع إلكتروني أو قاعدة بيانات أو خادم داخلي.

ه. اختراق مواقع الجامعة:



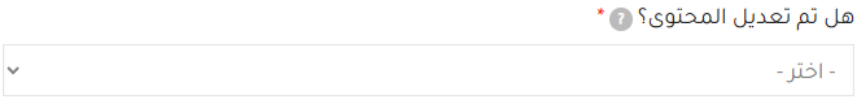
اختراق مواقع الجامعة

- عنوان الموقع أو الخدمة:



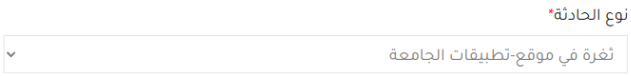
كتابة عنوان الموقع أو اسم الخدمة الذي تم اختراقه لتسهيل عملية التحقق والمعالجة.

- هل تم تعديل المحتوى؟



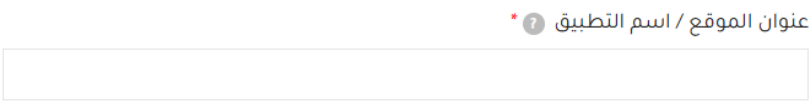
يرجى تحديد ما إذا تم ملاحظة أي تعديل أو تغيير في محتوى الموقع أو التطبيق بعد الاختراق.

و. ثغرة في موقع – تطبيقات الجامعة:



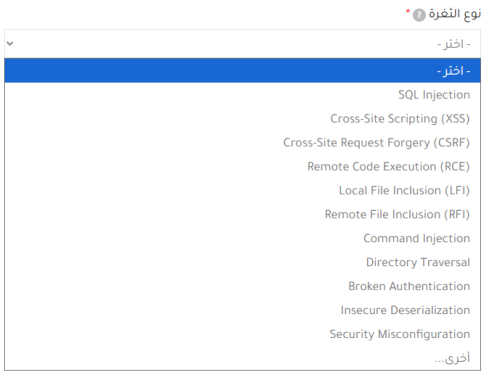
ثغرة في موقع / تطبيقات الجامعة

- عنوان الموقع أو اسم التطبيق:



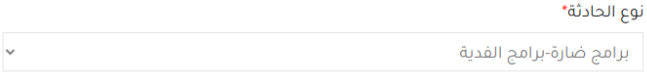
كتابة عنوان الموقع أو اسم الخدمة التي تم اكتشاف الثغرة فيها لتسهيل عملية التحقق والمعالجة.

- نوع الثغرة:



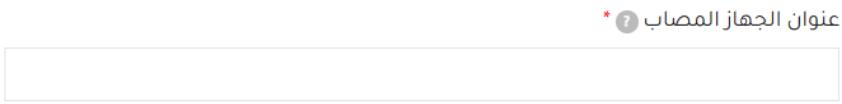
اختيار نوع الثغرة الأمنية من القائمة، وفي حال اختيار " أخرى" يرجى كتابة اسم الثغرة بشكل واضح في الحقل المخصص.

ز. برامج ضارة – برامج فدية:



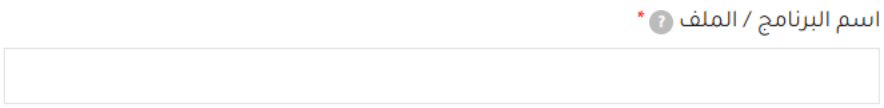
برامج ضارة / برامج الفدية

- عنوان الجهاز المصاب:



إدخال عنوان الـ IP الخاص بالجهاز المصاب بالبرنامج الضار أو برنامج الفدية.

- اسم البرنامج أو الملف:

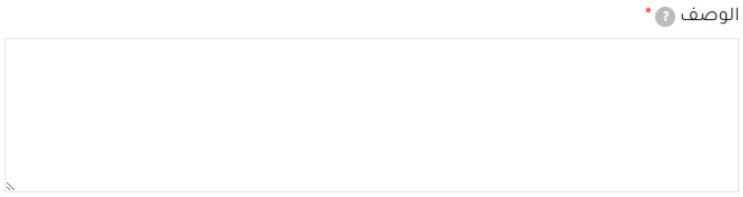


اسم البرنامج الضار أو برنامج الفدية الذي تم اكتشافه على الجهاز المصاب.

7- أولوية البلاغ:

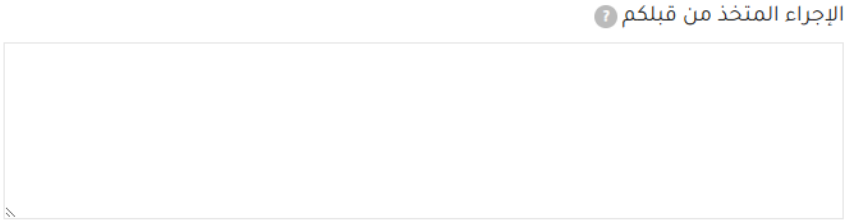
يتم اختيار أولوية البلاغ على الحادثة للمساعدة في سرعة الاستجابة واتخاذ الإجراء المناسب.

8- الوصف:



يرجى كتابة وصف واضح للحادثة يشمل ما حدث وأبرز ما تم ملاحظته من تأثير أو تغييرات على الأنظمة أو الخدمات.

9- الإجراء المتخذ من قبلكم:



يرجى توضيح جميع الإجراءات التي تم اتخاذها للتعامل مع الحادثة قبل إرسال هذا البلاغ، مع ذكر التفاصيل بشكل واضح ودقيق لتسهيل عملية المتابعة.