نتائج الشرق الأوسط

mimecast

حالة أمان البريد الإلكتروني للعام 2020

النتائج الرئيسية على مدار الأشهر الـ 12 الماضية

%67
من المؤسسات تأثرت ببرامج الفدية الضارة في الأشهر الـ 12 الماضية

%53
شهدَت ارتفاعًا في هجمات التصيّد الاحتيالي

%74
من المؤسسات تعتقد أن كلمة المرور الضعيفة تشكّل خطرًا أمنيًا كبيرًا

%48
من المؤسسات واجهَت خسارة في البيانات بسبب النقص في الجهوزية للمرونة الإلكترونية

%56
من المؤسسات شهدَت ارتفاعًا في عمليات الاحتيال في السنة الماضية

%79
من المؤسسات اختبرت تعطّلاً جراء الهجمات

%31
من المؤسسات لا تقدّم تدريبًا حول التوعية بشكل متكرر

%68
من المؤسسات تعتقد أن حجم تزييف هوية الويب أو البريد الإلكتروني سيبقى على حاله أو سيرتفع في السنة القادمة

%79
من المؤسسات التي أجابت على الاستطلاع قد تعرّضت لهجوم انتشر من مستخدم متضرر إلى موظفين آخرين

هجمات البريد الإلكتروني والسبب وراء عدم انخفاضها

%67
من المؤسسات تعتقد أنه من المرجّح أو المؤكّد أن تتعرّض لهجمات منقولة في البريد الإلكتروني في السنة القادمة

%62
من المؤسسات التي أجابت على الاستطلاع اعتبرَت أن عمليات التصيّد الاحتيالي بقيت كما هي أو حتى تزايدت

%62
من المؤسسات التي أجابت على الاستطلاع شهدَت على تزايد عمليات الاحتيال أو بقائها كما هي

%67
من الشركات تأثرت ببرامج الفدية الضارة. وواجهت يومَين من التعطّل.

من المؤسسات التي وقعت ضحية هجوم منقول في البريد الإلكتروني:

- **%48** واجهَت خسارة في البيانات
- **%31** عانت من الأثر على إنتاجية الموظفين
- **%25** شهدَت توقفًا/تعطلاً في الأعمال

في المتوسط

6/10
من المؤسسات تملك نظامًا أمنيًا لحماية رسائل البريد الإلكتروني الداخلية والصادرة:

- **%43** من المؤسسات لا تملك نطامًا لمراقبة أو الحماية من الهجمات المنقولة في البريد الإلكتروني أو تسرّبات البيانات في رسائل البريد الإلكتروني الداخلية.
- **%32** من المؤسسات لا تملك نطامًا لمراقبة أو الحماية من الهجمات المنقولة في البريد الإلكتروني مثل البرامج الضارة والارتباطات الضارة في البريد الإلكتروني الصادر.
- **%36** من المؤسسات لا تملك نطامًا لمراقبة أو الحماية من تسرّبات البيانات أو نقلها بشكل غير مصرّح به في البريد الإلكتروني الصادر.
- **%35** من المؤسسات لا تملك أداة للكشف عن أو لإزالة رسائل البريد الإلكتروني الضارة أو غير المرغوب فيها التي أصبحت في علبة الوارد لدى الموظفين.

كيفية فهم الحالة بفضل التدريب حول الوعي الأمني

%74
من المؤسسات تعتقد أن كلمة المرور الرديئة تشكّل خطرًا

%71
من المؤسسات تقول أن تسرّبات البيانات غير المقصودة تشكّل خطرًا كبيرًا

%79
من المؤسسات تعرّضت لنشاط ضار انتشر من موظف إلى آخر

%37
من المؤسسات تقدّم التدريبات شهريًا

%9
من المؤسسات لا تقدّم التدريب سوى مرة واحدة كل سنة

%100 من المؤسسات تقدّم بعض التدريبات بوتيرات وتنسيقات مختلفة:

- **%68** جلسات تدريب جماعية
- **%50** نصائح مطبوعة أو مُرسلة عبر البريد الإلكتروني
- **%49** اختبارات عبر الإنترنت
- **%60** تدريب شخصي

38% من التدريب تم تطويره داخل الشركة. **18%** من المؤسسات فقط تستخدم فيديوهات تدريبية. **17%** من المؤسسات فقط تستعين بجهة خارجية واحدة لتقديم التدريب.

الولاية الجديدة: حماية العلامة التجارية عبر الإنترنت

%53
من المؤسسات تتوقّع ارتفاعًا في عمليات تزييف هوية الويب أو البريد الإلكتروني واستغلال العلامة التجارية

7
متوسط عدد هجمات تزييف هوية الويب أو البريد الإلكتروني التي تكون المؤسسات على دراية بها

- **%74** من المؤسسات تشعر بالقلق حيال هجمات تزييف هوية مجال الويب أو الموقع أو استغلال العلامة التجارية
- **%76** من المؤسسات قلقة حيال هجمات قائمة على تزييف هوية مجال البريد الإلكتروني مباشرة

%99
من المؤسسات التي أجابت على الاستطلاع كانت على دراية ببروتوكول DMARC

%37
من المؤسسات تستخدم DMARC

%99
من المؤسسات خصصت ميزانية لوضع استراتيجيات بهدف حماية العلامة التجارية

من هي الجهة المسؤولة عن الميزانية؟

%47 المدير التنفيذي لتكنولوجيا المعلومات
%41 المدير التنفيذي الأمني لتكنولوجيا المعلومات
%41 المدير التنفيذي المالي
%14 المدير التنفيذي التسويقي
%12 قسم الشؤون القانونية/الامتثال

** من المرجح أكثر أن يكون المدير التنفيذي المالي هو المسؤول عن الميزانية في المملكة العربية السعودية، مقارنة بالكثير من المناطق الأخرى حيث تم إجراء الاستطلاع*

هل المرونة الإلكترونية في تحسّن؟

%82
من المؤسسات التي أجابت على الاستطلاع تملك استراتيجية حول المرونة الإلكترونية أو تقوم بطرح استراتيجية بشكل نشط

%18
من المؤسسات ما زالت تخطط لتنفيذ استراتيجية حول المرونة الإلكترونية

%96
من المؤسسات تستخدم Office 365 كموفر البريد الإلكتروني الخاص بها

%40 من المؤسسات توافق بشدّة على أن **Office 365** يقدّم أمانًا على المستوى العالمي
%73 من المؤسسات واجهَت انقطاعًا في خدمة **Office 365** في الأشهر الـ **12** الماضية
%78 من المؤسسات أضافت أو تقوم حاليًا بإضافة طبقات إضافية من الاستمرارية والمرونة الإلكترونية

يؤدّي النقص في الجهوزية للمرونة الإلكترونية إلى:

- **%48** خسارة في البيانات
- **%31** أثر سلبي على إنتاجية الموظفين
- **%25** تعطّل الأعمال

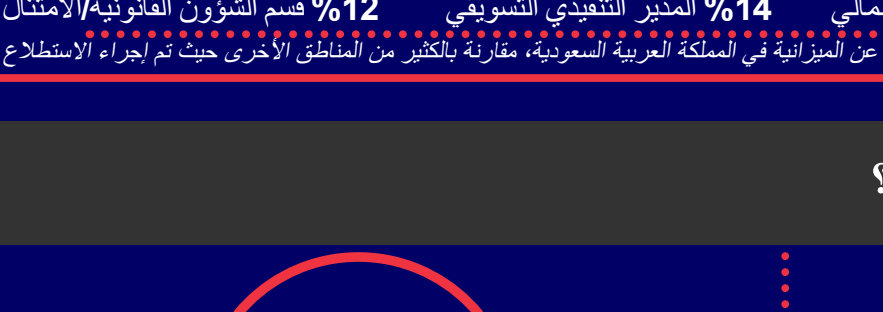
ما المضمّن في استراتيجياتها المتعلّقة بالمرونة الإلكترونية؟

- **%72** أمان البريد الإلكتروني
- **%63** أمان الشبكة
- **%68** أمان الويب
- **%69** نسخ احتياطي/استرداد البيانات

2/5
من المؤسسات اعتمدت اختبار الاختراق للأنظمة الأساسية، وتقوم باختبار عمليات الاستجابة للحوادث بشكل منتظم

1/2
من المؤسسات اعتمدت حماية استغلال العلامة التجارية في ما يتعلّق بتزييف هوية البريد الإلكتروني ومجال الموقع الإلكتروني

تنزيل التقرير الكامل



احصل عليه الآن

mimecast.com/state-of-email-security

mimecast