هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

هيئة الاتصالات وتقنية المعلومات

تقييم الوضع الراهن للرسائل الاقتحامية
في المملكة العربية السعودية

جدول المحتويات

١- الغرض من هذه الوثيقة ٣
٢- منهجنا في الدراسة ٤
٣- ملخص تنفيذي ٥
٤- تحديد الأطراف ذات العلاقة ٨
٤-١ تحليل دورة حياة نشاط الرسائل الاقتحامية ٨
٤-٢ الحصول على المعلومات الشخصية ٨
٤-٣ الأطراف ذات العلاقة المستخدمة كوسط لإرسال الرسائل الاقتحامية ٩
٤-٤ الأطراف ذات العلاقة المستضيفة لخدمات البريد الإلكتروني ١٠
٤-٥ التبليغ عن الرسائل الاقتحامية للجهات ذات العلاقة ١٢
٤-٦ تنفيذ العقوبة من الجهات ذات العلاقة ١٣
٤-٧ الخاتمة ١٤
٥- الردود الواردة من الجهات ذات العلاقة ١٦
٥-١ مؤسسة النقد العربية السعودي ١٦
٥-٢ مقدمو خدمات المعطيات ١٦
٥-٣ مقدمو خدمة الجوال ١٧
٥-٤ المرخصون لإرسال الرسائل القصيرة الجماعية الاقتحامية ١٧
٥-٥ مزودو الحلول ١٨
٥-٦ مقدمو خدمة الإنترنت ١٨
٥-٧ الشركات ١٩
٥-٨ الجامعات ١٩
٥-٩ وزارة الداخلية ٢٠
٥-١٠ هيئة الاتصالات وتقنية المعلومات ٢٠
٥-١١ مدينة الملك عبدالعزيز للعلوم والتقنية / وحدة خدمات الإنترنت ٢٠
٥-١٢ الاهتمامات الرئيسية للأطراف ذات العلاقة وتوصياتها ٢١
٦ نتائج المسح باستخدام استمارات استطلاع الرأي ٢٤
٦-١ تعريف الرسائل الاقتحامية ٢٤
٦-٢ حجم المشكلة ٢٤
٦-٣ الطريقة المتبعة حالياً من الجهات ذات العلاقة لمكافحة الرسائل الاقتحامية ٣٠

١- الغرض من هذه الوثيقة

الغرض من هذه الوثيقة هو عرض نتائج الدراسة التي أجريت للتأكد من حجم الرسائل الاقتحامية(SPAM) في المملكة العربية السعودية. وتم من خلال تلك الدراسة التركيز على تكوين فهم جيد لمشكلة الرسائل الاقتحامية (SPAM) في المملكة.

وقد تم إعداد هذه الوثيقة باستخدام الإحصاءات التي تم تجميعها من الأطراف ذات العلاقة باستخدام عدد من الوسائل المختلفة منها استبيانات استطلاع الرأي، والمقابلات الشخصية، والاجتماعات. وتغطي هذه الدراسة الرسائل الاقتحامية (SPAM)المتعلقة بالبريد الإلكتروني الجوال والفاكس. كما تلقى هذه الدراسة الضوء على بعض اهتمامات وتوصيات الأطراف ذات العلاقة فيما يتعلق بالرسائل الاقتحامية، وكذلك التدابير المتخذة من قبل تلك الأطراف لضبط والسيطرة على الرسائل الاقتحامية (SPAM) في شبكاتها.

٢- منهجنا في الدراسة

لقد اتبعنا منهجاً يتكون من ثلاث خطوات في تجميع المعلومات المطلوبة عن حالة الرسائل الاقتحامية في المملكة، وهذه الخطوات هي كالتالي:

- الاتفاق على تعريف أولي للرسائل الاقتحامية (SPAM) ، يمكن استخدامه كأساس لتجميع المعلومات.
- تحديد والاتفاق على المصادر المحتملة للحصول على إحصاءات تتعلق بالرسائل الاقتحامية والأطراف ذات العلاقة الذين يمكن أن يمدوا يد العون في هذا الصدد.
- تجميع الإحصاءات المتعلقة بالرسائل الاقتحامية من الأطراف ذات العلاقة التي تم تحديدها.

وتتضمن الفقرات التالية وصفاً أكثر تفصيلاً لكل خطوة من هذه الخطوات:

تعريف الرسائل الاقتحامية والمؤشرات المتعلقة بتلك الرسائل

تم تعريف الرسائل الاقتحامية في بحثنا على أنها الرسائل الجماعية غير المطلوبة المحتوية على محتويات تجارية أو مسيئة أو مرفوضة والتي يتم إرسالها بشكل جماعي إلى الأشخاص دون موافقتهم من خلال البريد الإلكتروني أو الفاكس أو الرسائل الفورية مثل الرسائل القصيرة. علماً بأن مؤشر الرسائل الاقتحامية (SPAM)الأساسي المستخدم هو "معدل الرسائل الاقتحامية" والذي يعرّف بأنه نسبة الرسائل الاقتحامية (SPAM)مقارنة بإجمالي عدد الرسائل المستلمة.

تحديد مصادر الإحصاءات المتعلقة بالرسائل الاقتحامية

تم تحديد المصادر الرئيسية ذات العلاقة التي تعتبر مناسبة لتجميع الإحصاءات المتعلقة بالرسائل الاقتحامية (SPAM)في المملكة والتبليغ عنها، وهي المؤسسات القادرة على الإفادة عن حجم الرسائل الاقتحامية (SPAM)المستلمة أو التي تم تصفيتها كنسبة من إجمالي عدد رسائل البريد الإلكتروني المستلمة. وقد تم كذلك الأخذ في الاعتبار مقدمة خدمات الإنترنت الذين يستخدمون أدوات إلكترونية لتصفية الرسائل الاقتحامية (SPAM)والقادرين على تقديم تقارير عن الرسائل الاقتحامية (SPAM)التي تم تصفيتها من خلال الأدوات المستخدمة لديهم كنسبة من إجمالي رسائل البريد الإلكتروني. أما فيما يتعلق بالرسائل القصيرة المصنفة كرسائل اقتحامية، فقد تم الأخذ في الاعتبار مقدمي خدمة الجوال الذين يملكون بوابات إلكترونية (Gateway) و/أو خوادم (Servers)، والتي يتم من خلالها تسليم الرسائل القصيرة الاقتحامية.

تجميع الإحصاءات المتعلقة بالرسائل الاقتحامية

يعد تحديد المؤشرات الأساسية للرسائل الاقتحامية والمصادر المحتملة للبيانات المتعلقة بتلك الرسائل، تم اتباع عدة طرق لتجميع البيانات المتعلقة بالرسائل الاقتحامية. وتعتمد الطريقة المتبعة على نوع تلك الرسائل الاقتحامية. بالنسبة للرسائل الاقتحامية الخاصة بالبريد الإلكتروني، كانت الطريقة الرئيسية المستخدمة في تجميع البيانات هي استمارات استطلاع الرأي والمقابلات الشخصية التي استهدفت مؤسسات مختارة ومزودي خدمة الإنترنت. وتم إجراء بعض المقابلات والمناقشات مع مقدمي خدمة خارجيين مثل مقدمي الحلول الأمنية للحصول على ما لديهم من معلومات حول الرسائل الاقتحامية. أما بالنسبة للرسائل الاقتحامية المتعلقة بالرسائل القصيرة، فقد كانت الطريقة الرئيسية المستخدمة في تجميع البيانات هي استمارات استطلاع الرأي والمقابلات الشخصية التي استهدفت الرسائل القصيرة الجماعية ومقدمي خدمة الجوال للحصول على المعلومات المتعلقة بالرسائل القصيرة المصنفة كرسائل اقتحامية. وتم كذلك تجميع بعض الإحصاءات الإضافية من قبل مقدمي الخدمة من خلال بوابات الرسائل القصيرة لديهم حول عدد الرسائل القصيرة المستلمة من قبل الهواتف الجوالة في المملكة.

٣- ملخص تنفيذي

تمثل الرسائل الاقتحامية (SPAM)إزعاجاً وتهديداً رئيسياً لمستخدمي تطبيقات تقنية المعلومات والاتصالات، وتنتشر عبر كافة وسائل الاتصالات. وكما هو الحال في العديد من الدول والمنظمات والهيئات وفرق العمل الإقليمية والدولية التي اتخذت خطوات للتعامل مع المشاكل والقضايا الناشئة عن الرسائل الاقتحامية، فقد اتخذت المملكة العربية السعودية المبادرات لتطوير هيكلية تنظيمية لمكافحة الرسائل الاقتحامية. وبناء على ذلك، وإلى جانب الأخذ في الاعتبار خبرات الدول الأخرى وتوصيات الهيئات والمنظمات الدولية، فإنه من الضروري تقييم الحالة الراهنة للرسائل الاقتحامية في المملكة.

يهدف هذا التقرير إلى وصف نتائج الدراسة التي أجريت لتحديد حجم الرسائل الاقتحامية (SPAM)في المملكة، بما في ذلك استخدامها لأغراض خبيثة كالتزوير والاحتيال (phishing) ونشر الفيروسات (Viruses). ويهدف التقرير كذلك إلى التوعية بالرسائل الاقتحامية (SPAM)والتدابير المتبعة حالياً لمكافحة الرسائل الاقتحامية (SPAM)وأثرها على الأطراف ذات العلاقة في المملكة. ويعتبر قياس الرسائل الاقتحامية (SPAM)بمثابة المفتاح لتقييم مدى انتشار هذه الرسائل وفعالية الإطار التنظيمي الخاص بمكافحتها في المملكة.

ولتحقيق هذا الغرض، تم تحديد جميع الأطراف ذات العلاقة ووضع إطار تنظيمي لتجميع الإحصاءات المتعلقة بالرسائل الاقتحامية، ويشمل هذا الإطار البريد الإلكتروني ورسائل الجوال القصيرة (SMS) والفاكس، والتركيز على ثلاثة جوانب: **الأول** تعريف الرسائل الاقتحامية (SPAM)ومؤشراتها، حيث تم تعريف عبارة "معدل الرسائل الاقتحامية" على أنها نسبة الرسائل الاقتحامية (SPAM)إلى إجمالي عدد الرسائل المستلمة. **والثاني**، تحديد المصادر التي يمكن الحصول منها على الإحصاءات المتعلقة بالرسائل الاقتحامية، إضافة إلى لما يمكن الحصول عليه من خلال المقابلات الشخصية وأدوات تصفية ومكافحة الرسائل الاقتحامية (SPAM)المستخدمة من قبل المنظمات ومزودي خدمة الإنترنت، وهما المصدران الرئيسيان لتحديد رسائل البريد الإلكتروني الاقتحامية، بينما تم استخدام البوابات الإلكترونية والخوادم (Servers) المملوكة من مزودي خدمات الجوال لحساب الرسائل النصية القصيرة الاقتحامية. **والثالث**، تجميع الإحصاءات المتعلقة بالرسائل الاقتحامية، وتم ذلك من خلال معاينة البيانات المنشورة الموثوقة، وكذلك من خلال المسح الميداني والمقابلات الشخصية والمناقشات مع الأشخاص المعنيين بما في ذلك هيئة الاتصالات وتقنية المعلومات (CITC)، ومدينة الملك عبدالعزيز للعلوم والتقنية، ووزارة الاتصالات وتقنية المعلومات (MCIT)، ووزارة الداخلية (MOI)، ومؤسسة النقد العربي السعودي(SAMA)، والشركات والمؤسسات المالية، ومقدمي خدمة الإنترنت، ومقدمي خدمة المعطيات، والأطراف المرخص لهم بإرسال الرسائل النصية القصيرة الجماعية، ومشغلي خدمة الجوال، ومقدمي الحلول، وغيرهم.

وعلى الرغم من اختلاف معدلات الرسائل الاقتحامية (SPAM)بحسب الموقع الذي يتم القياس فيه، إلا أن هذه الرسائل تمثل مشكلة خطيرة في المملكة. وبناء على المعلومات التي جمعها مقدمو خدمة الإنترنت، فإن معدل رسائل البريد الإلكتروني الاقتحامية في المملكة كان ٥٤%. بينما أفادت مصادر أخرى، كموردي منتجات مكافحة الرسائل الاقتحامية، أن نسبة تلك الرسائل تتراوح بين ٤٠% - ٦٠%. وعلى سبيل المثال، فإن التقارير المنقولة عن سيمانتيك (Symantec) تفيد أن نسبة الرسائل الاقتحامية (SPAM)كانت ٥٩% في عام ٢٠٠٦م، بينما أفادت تقارير (Message Labs) أن الرسائل الاقتحامية (SPAM)في عام ٢٠٠٦م شكلت ٤٨% وفي عام ٢٠٠٧م (لغاية يوليو) شكلت ٤٣% من إجمالي عدد الرسائل المستلمة. وفي المقابل فإن الرسائل الاقتحامية (SPAM)المرسلة بالفاكس لم تعتبر بأنها مصدر رئيسي للرسائل الاقتحامية، ومعدل إرسالها يقل عن ٦%. وتشكل الرسائل التسويقية المباشرة النوع الرئيسي من الرسائل الاقتحامية (SPAM)المستلمة في المملكة، وهذا يعكس الأغلبية العظمى للرسائل الاقتحامية التجارية على مستوى العالم. وبالنسبة للرسائل القصيرة الاقتحامية، فقد أفاد مشغلو خدمة الجوال أنها تشكل ما معدله ١,٧%، حيث أن ٦٥% من هذه الرسائل النصية القصيرة هي تجارية، ٢٠% بذيئة، ٢% سياسية، ٣% دينية، ٥% تتعلق بأسواق الأسهم و٥% ذات أغراض أخرى. ويلخص الجدول التالي النتائج الرئيسية للدراسة.

	معدل رسائل البريد الإلكتروني الاقتحامية	النسبة الأكبر من الرسائل الاقتحامية	معدل رسائل الفاكس الاقتحامية	معدل الرسائل القصيرة الاقتحامية	استخدام القوائم السوداء RBLs	نسبة استخدام أدوات مكافحة الرسائل الاقتحامية
المعدل	54%	تجارية	6%	1.7%[1]	17%	83%

إن رسائل البريد الإلكتروني الاقتحامية، إضافة لكونها تشكل إزعاجاً للأشخاص، فإنها تسبب مشاكل أخرى تتعلق بالسعة وعرض النطاق الترددي وأداء الموظفين. وترى معظم الشركات أن الأثر الأساسي للرسائل الاقتحامية كان على موارد خادم البريد الإلكتروني والشبكة وإضاعة الوقت، بينما يرى مقدمو خدمة الإنترنت أن عملاؤهم هم الطرف الأكثر تأثراً بالرسائل الاقتحامية، كما أن هناك تأثراً كبيراً على عرض النطاق الترددي والإنتاجية.

وبالنظر لأثر الرسائل الاقتحامية (SPAM)في المملكة، يبدوا أن معظم الشركات/ المؤسسات، باستثناء البنوك، لا تبذل جهداً كبيراً في تثقيف وتعليم موظفيها وعملائها حول كيفية التعامل مع الرسائل الاقتحامية، بينما تقدم جميع البنوك برامج توعية لموظفيها وعملائها.

ومن الملاحظ أن ٨٣% من الأطراف ذات العلاقة لديها أدوات لمكافحة الرسائل الاقتحامية. ومما تجدر ملاحظته أن مزودي خدمات الإنترنت يركزون على تصفية حركة مرور رسائل البريد الإلكتروني الواردة عبر خوادم (Mail Gateways) البريد الإلكتروني الموجودة في مركز بيانات مزود الخدمة، ولا يقوم مقدمو الخدمة بتصفية جميع الحركة المرورية (وخصوصاً الرسائل الصادرة) نظراً للقيود الحالية على الميزانيات والموارد ونقص الموظفين القادرين فنياً. وفي حقيقة الأمر، فإن مزودي خدمة الإنترنت المستخدمين للقوائم السوداء (RBLs) أفادوا بتعرضهم لمعدلات أقل من الرسائل الاقتحامية.

وفي ظل عدم وجود عمليات تبليغ وتقديم تقارير رسمية للشكاوى، فلا عجب في أن معظم المؤسسات تتعامل مع الرسائل الاقتحامية (SPAM)داخلياً أو حتى تتجاهل الشكاوى المتعلقة بتلك الرسائل. وفي المقابل، فإن الأمر يختلف في حالة البنوك، حيث أنه يوجد لدى ٥٠% منهم إجراءات للتبليغ عن الشكاوى المتعلقة بالتزوير والاحتيال إلى هيئة الاتصالات وتقنية المعلومات (CITC) أو لمؤسسة النقد العربي السعودي(SAMA).

وعندما يتعلق الأمر بهذا القطاع، فقد اتضح أنه لا توجد لائحة للضوابط السلوكية لدى مزودي خدمات الإنترنت أو التسويق الإلكتروني في المملكة. كما أن معظم مزودي الخدمة لم يضمّنوا أي أحكام في سياسات الاستخدام المعتمدة تغطي قضية الرسائل الاقتحامية.

وبناء على توصيات الهيئات الدولية المطلعة جيداً على هذه المشكلة، فإنه من أجل مكافحة الرسائل الاقتحامية (SPAM)يجب تناول عدة جوانب مثل الجوانب القانونية وآلية التنفيذ والجوانب الفنية والوعي والمساعدة من القطاع وغير ذلك. وبحسب إفادة معظم الأطراف ذات العلاقة، فإن الجانب القانوني هو الأكثر أهمية في مكافحة الرسائل الاقتحامية (SPAM)في المملكة، بينما وجود لائحة مناسبة للضوابط السلوكية بين مزودي الخدمة سيساعد بصورة جوهرية على منع تلك الرسائل.

وحسبما ورد في الدراسة، فإن الرسائل الاقتحامية (SPAM)تمثل مشكلة خطيرة نظراً لما تنطوي عليه من إزعاج للأشخاص والمؤسسات ومقدمي الخدمات. وكما تقدم ذكره، هناك وعي ضئيل بالرسائل الاقتحامية، ولا توجد قواعد أو ضوابط سلوكية تحكم عمل مقدمي الخدمات والمزاولين للتجارة الإلكترونية. وإضافة لذلك، فإن الاشتراطات المقدمة من خلال التراخيص الممنوحة لمقدمي خدمة الإنترنت ومقدمي خدمات الرسائل الجماعية ومقدمي خدمة البلوتوث (Bluetooth) لا يتم مراجعتها وتدقيقها، ولا توجد آلية للتأكد من التزام الأطراف ذات الصلة بتنفيذها.

كل ما تقدم يبرر الحاجة إلى تطوير هيكلية عامة لمكافحة الرسائل الاقتحامية (SPAM)في المملكة. وبتطوير هذه الهيكلية لمكافحة الرسائل الاقتحامية (SPAM)مقرونة بآلية تنفيذ قوية، والتأكد من الحصول على مساندة القطاع المعني، وتقديم

[1] تستند هذه النسبة إلى التعريف الوارد في لائحة الضوابط السلوكية لدى النظام العالمي للهواتف المتنقلة GSMA

برامج التوعية وتنفيذ الحلول الفنية والمراقبة المستمرة لمعدلات الرسائل الاقتحامية، والتركيز على السيطرة على الرسائل الاقتحامية (SPAM)التجارية، فإنه يمكن تقليل الرسائل الاقتحامية (SPAM)إلى حد بعيد في المملكة.

٤- تحديد الجماعات ذات العلاقة

٤-١ تحليل دورة حياة نشاط الرسائل الاقتحامية

يتناول هذا التحليل دورة الحياة النموذجية لنشاطات الرسائل الاقتحامية، وتتمثل هذه الدورة بما يلي:

١) يتم الحصول على عنوان المستلم (بريده الإلكتروني أو رقم فاكسه أو رقم جواله) ومن ثم تخزينه في مستودع بيانات لغرض محدد.
٢) يحصل مرسل الرسائل الاقتحامية (SPAM)على تفاصيل محددة للعنوان، تستخدم بعد ذلك في أنشطة الرسائل الاقتحامية.
٣) يتم نقل الرسائل الاقتحامية (SPAM)من خلال وسط محدد (مقدمي خدمة الإنترنت، مقدمي خدمات الجوال، إلخ).
٤) تُستلم الرسالة بواسطة مستضيف البريد (مقدم خدمة البريد، البنوك، إلخ).
٥) يستلم المستخدم النهائي (المستلم) الرسالة.
٦) يقوم المستلم بالتبليغ عن الرسالة الاقتحامية إلى الجهة المختصة إذا كان مطلوباً منه ذلك.
٧) تتولى الجهة المختصة تطبيق النظام (المحاكمة وصدور الحكم).

يظهر الشكل التالي الأطراف الرئيسية ذات العلاقة المشاركة في مراحل دورة حياة نشاط الرسائل الاقتحامية. وهذه المراحل السبع موضحة في الشكل التالي:

وتشتمل الأقسام التالية على أوصاف وشروحات لنماذج من بعض مجموعات الأطراف ذات العلاقة المذكورة في الشكل أعلاه، بالإضافة إلى وصف المراحل المختلفة من دورة حياة الرسائل الاقتحامية:

٤-٢ الحصول على المعلومات الشخصية

العديد من المؤسسات كالبنوك وتجار التجزئة ومقدمي خدمة الإنترنت ومقدمي خدمة الجوال والاتصالات ومزودي خدمة البريد وغيره يستخلصون بيانات العملاء والمشتركين ويحفظونها في أنظمتهم، حيث يتم الحصول على البيانات في الغالب لأغراض محدده، وتتم الموافقة على ذلك بشكل نمطي وروتيني من قبل الشخص المعني. والعديد من هذه المؤسسات لديها سياسات سرية داخلية تمنعها من استخدام المعلومات لأي غرض كان باستثناء الغرض الذي من أجله تم الحصول على المعلومات. وفي بعض الحالات، فإن العديد من هذه المؤسسات قد تطلب من الشخص المعني الموافقة

رسمياً على استخدام معلومات الاتصال هذه لأغراض التسويق الإلكتروني. وبعض هذه المؤسسات قد تبيع معلومات الاتصال الخاص بالمشتركين إلى أطراف أخرى لاستخدامها لغرض إرسال الرسائل الاقتحامية.

إن توفر معلومات الاتصال والمعلومات الشخصية هذه المخزنة لدى تلك المؤسسات يعد في الغالب المصدر الرئيسي لمعلومات الاتصال بالنسبة لمرسلي الرسائل الاقتحامية.

٤-٣ الجماعات ذات العلاقة المستخدمة كوسط لإرسال الرسائل الاقتحامية

بعد تجميع المعلومات اللازمة، يقوم مرسل الرسائل الاقتحامية (SPAM)بإرسال تلك الرسائل إلى الأشخاص المستهدفين عبر وسط معين، وقد يختلف الوسط المستخدم لهذا الغرض. وقد يتم استخدام وسط مملوك لأحد الجماعات ذات العلاقة مثل مقدمي خدمة الإنترنت ومقدمي خدمة الجوال ومقدمي خدمة المعطيات ومقدمي خدمة الرسائل القصيرة الجماعية وغيرهم. وهذه الجماعات ذات العلاقة هي في حقيقة الأمر معنية بالأمر، لأن مالك الوسط المرسلة عبره الرسائل الاقتحامية (SPAM)قد يوفر بمعرفته أو بدون معرفته المنصة (Platform) اللازمة لمرسلي الرسائل الاقتحامية (SPAM)للقيام بنشاطاتهم.

الجهة ذات العلاقة	السبب	أمثلة
مقدمو خدمة الإنترنت	مقدمو خدمة الإنترنت هم ناقلون للاتصالات الإلكترونية، وبشكل رئيسي رسائل البريد الإلكتروني. يمكن لمقدمي خدمة الإنترنت إعطاء مرسلي الرسائل الاقتحامية (SPAM)الوسيلة التي يستخدمونها في إرسال تلك الرسائل. كما أنهم يشكلون - بشكل عام - أول نقطة اتصال من قبل المستلمين عندما بدأو في ملء صناديق الوارد لديهم بالرسائل المتطفلة. تعتبر مجهودات مقدمي خدمة الإنترنت ضرورية للحد من كمية الرسائل الاقتحامية (SPAM)والمتطفلة من خلال تطبيق تدابير تصفية مناسبة في خوادم (Mail Gateways) البريد الإلكتروني لديهم.	• شركة نسما الوطنية للتقنية المتقدمة المحدودة (نسما). • برنامج سلطان بن عبدالعزيز للاتصالات الطبية والتعليمية (ميدو نت MeduNet) • الشركة العربية لخدمات الإنترنت والاتصالات (أول نت). • شركة الاتصالات السعودية (سعودي نت).
مقدمو خدمات الهاتف الجوال	يمكن استخدام رسائل الجوال القصيرة (SMS) كشكل آخر من أشكال الرسائل الاقتحامية (SPAM)مثلما هو موضح سابقاً في الإحصائيات.	• شركة الاتصالات السعودية • شركة اتحاد اتصالات (موبايلي)
مقدمو خدمات البيانات	تنفيذ أي ضوابط محتملة على مستوى مقدمي خدمة البيانات يمكن أن يعيق من تدفق الرسائل الاقتحامية (SPAM)الواردة والصادرة.	• شركة الاتصالات السعودية • بيانات العلا لخدمات الشبكات (بيانات كونسورتيوم).

الجهة ذات العلاقة	السبب	أمثلة
مقدمو خدمات الرسائل الجماعية	تشكل رسائل الجوال القصيرة (SMS) الجماعية شكلاً رئيسياً من أشكال الرسائل الاقتحامية، علماً أن هذه الرسائل تُستخدم للترويج للبضائع والخدمات والمبيعات وخلافه.	• شركة إيكول بلس المحدودة eCallPlus Ltd • شركة مدياكول المحدودة.
هيئة الاتصالات وتقنية المعلومات (CITC).	تقوم هيئة الاتصالات وتقنية المعلومات (CITC) بإدارة البوابات الإلكترونية على مستوى المملكة. جميع محتويات الإنترنت التي يتم مشاهدتها من داخل المملكة تخضع للتصفية بغية التحقق من المحتويات التي تتعارض مع القيم أو الأنظمة الوطنية المرعية في المملكة العربية السعودية. يُحظر الوصول إلى المواقع الإباحية، وتعمل هيئة الاتصالات وتقنية المعلومات (CITC) بصفة دائمة على التخلص من هذه المواقع، وفي ذات الوقت، تقوم بمراقبة الفئات الأخرى من المواقع ولكن بدرجة أقل تشدُّداً، ومنها المواقع المتعلقة بالمخدرات، الكحول، الميسر، الإرهاب، التزوير والاحتيال، علاوة على المواقع المتطرفة سياسياً أو دينياً.	• هيئة الاتصالات وتقنية المعلومات.
مقدمو خدمة البريد الإلكتروني المجاني (يتم تأكيدها).	يتعامل مقدمو خدمة البريد الإلكتروني المجاني مع أكبر كميات من الرسائل الاقتحامية (SPAM)على مستوى العالم. وحيث أنه لا يوجد مقر لأي من مزودي هذه الخدمة في المملكة العربية السعودية، بالتالي يستطيع معظم الناس الحصول على منفذ لخدماتهم البريدية والتي يمكن استخدامها مجاناً لأي غرض كان.	• ياهو • هوت ميل • جي ميل • لايكوس Lycos

٤-٤ الجماعات ذات العلاقة المستضيفة لخدمات البريد الإلكتروني

عقب ذلك يتم استقبال الرسائل الاقتحامية (SPAM)بواسطة الجهة المستضيفة لصناديق البريد الخاصة بالمستلمين، علماً أن مستضيف البريد إما أن يكون مزود خدمة بريد أو مؤسسة تقدم خدمة البريد الإلكتروني للعاملين لديها. وهذه الأطراف المعنية لها صلة بهذا الأمر وذلك لأنها في الغالب تستخدم مرشحات (Filters) وأدوات لمراقبة الرسائل الاقتحامية (SPAM)الموجهة إلى المشتركين في خدماتها البريدية.

الطرف ذي العلاقة	السبب	أمثلة
مقدمو خدمة البريد	تقوم الشركات المستضيفة والمسكّنة لخدمات البريد الإلكتروني والمواقع الإلكترونية بتوفير خدمات البريد الإلكتروني إلى الشركات والأفراد مقابل رسوم، وليست	• يقوم معظم مقدمي خدمات الإنترنت بتوفير خدمات البريد كجزء من خدمات الاشتراك.

الطرف ذي العلاقة	السبب	أمثلة
	هناك تكلفة إضافية على عدد رسائل البريد الإلكتروني الواردة أو الصادرة من قبل المشتركين من هذه الشركات، ويمكن أن تشكل هذه الخدمات أرضية جيدة لمرسلي الرسائل الاقتحامية.	
الشركات	تعمل معظم الشركات على تشغيل خوادم (Mail Gateways) البريد الإلكتروني الخاصة بها. وعلى الرغم من احتمال وجود سياسة واضحة تمنع استخدام البريد الإلكتروني للشركة لغرض إرسال رسائل اقتحامية، لكن ما زال بإمكان البريد الإلكتروني للشركات إرسال رسائل بريد إلكتروني جماعية وتسلسلية. بالإضافة إلى ذلك، يتعين على الشركات معالجة الكميات الهائلة من الرسائل الاقتحامية (SPAM)التي ترد إليها عن طريق خوادم (Mail Gateways) البريد الإلكتروني التابعة لها، علماً أن الشركات تتأثر بشكل كبير بالرسائل الاقتحامية (SPAM)التي تهدر قدراً كبيراً من الجهد البشري وتفضي إلى فقد كبير للأموال.	• أرامكو • الشركة السعودية للصناعات الأساسية (سابك)
البنوك	إن البنوك هي شركات تجارية، والتي بالإضافة إلى ما يواجه كل الشركات من رسائل اقتحامية عبر البريد الإلكتروني، فهي أيضاً تتعرض إلى هجمات التزوير و التصيد (Phishing). إن رسائل التزوير و التصيد (Phishing) بالبريد الإلكتروني من المحتمل أن تلحق ضرراً بليغاً بعائدات البنك وسُمعته إذا لم تتم معالجتها بسرعة.	• مجموعة سامبا المالية (سامبا) • البنك السعودي البريطاني (ساب)
مقدمو الحلول الأمنية/مقدمو خدمات البنية التحتية	بينما يعمل مزودو الحلول الأمنية على توفير أدوات تصفية المحتويات ليتسنى التخلص من الرسائل الاقتحامية (SPAM)المحتملة قبل وصولها إلى المستخدم النهائي، فإن مزودي خدمات البُنى التحتية يضمّنون إمكانيات مكافحة الرسائل الاقتحامية (SPAM)في خصائص منتجاتهم.	• سيمانتيك • ميكروسوفت • أنظمة أمن الإنترنت بشركة آي بي أم
الجامعات	إن شبكات الجامعات معرضة بصفة عامة للمتطفلين والقراصنة Hackers الذين يستخدمون أجهزة الجامعات كشبكات لتشغيل برامج متطفلة عن بعد وبشكل تلقائي botnets، وبالتالي تصبح أجهزة الحاسب الآلي بالجامعات مكاناً خصباً وجاذباً لمرسلي الرسائل الاقتحامية (SPAM)لشن هجماتهم.	• جامعة الملك فهد للبترول والمعادن • جامعة الملك سعود

٤-٥ التبليغ عن الرسائل الاقتحامية للجماعات ذات العلاقة

عند يتلقى المستقبل رسائل اقتحامية، فقد يرغب في تبليغ وحدة تنظيمية مختصة في المملكة خاصة إذا لحق به ضرر جراء تلك الرسائل الاقتحامية.

وقد تختلف الوحدة المختصة التي يتم إبلاغها من المستلم بتلك الرسائل الاقتحامية (SPAM)بناء على نوع ومنشأ ومحتوى الرسالة الاقتحامية. فعلى سبيل المثال، يمكن لمستقبل الرسالة أن يبلّغ هذه الرسائل الاقتحامية (SPAM)إلى البنوك أو الشركة/الشركات التي يعمل/تعمل لديها أو الجهات الحكومية ذات الصلة، وتوجد أدناه قائمة بهذه الجماعات ذات العلاقة:

الطرف ذي العلاقة	السبب	أمثلة
	تتمتع هيئة الاتصالات وتقنية المعلومات (CITC) بالحق في حماية مصالح مستخدمي خدمات الاتصالات العامة والإنترنت، وكذلك باقتراح أنظمة ولوائح لها علاقة بقطاعات الاتصالات. عندما تقع انتهاكات الرسائل الاقتحامية (SPAM)ضمن نطاق "نظام التعاملات الإلكترونية" (مثل قضايا الخصوصية) أو ضمن نطاق "نظام مكافحة جرائم المعلوماتية" (مثل الوصول غير المصرح به إلى الحاسبات الآلية والشبكات) فإن الجهة التي يتعين على ضحايا الرسائل الاقتحامية (SPAM)إبلاغها هي هيئة الاتصالات وتقنية المعلومات (CITC).	• هيئة الاتصالات وتقنية المعلومات.
الجهات الحكومية	تقوم مؤسسة النقد العربي السعودي(SAMA) وهي البنك المركزي السعودي، بالإشراف على البنوك التجارية وإصدار الأنظمة واللوائح المصرفية. وفي حال إخفاق عملاء البنك في تأمين أموالهم أثناء عمليات الإنترنت (حدوث أعمال تزوير و تصيد باستخدام الرسائل الاقتحامية) فإن مؤسسة النقد العربي السعودي(SAMA) هي الجهة التي يتعين على عملاء البنوك إبلاغها، علماً بأن هناك لجنة لدى المؤسسة متخصصة في الفصل في النزاعات المصرفية بين البنوك وعملائها.	• مؤسسة النقد العربي السعودي
	قد تكون وزارة الداخلية (MOI) هي إحدى الجهات الحكومية التي يتعين على مستلمي الرسائل الاقتحامية (SPAM)إبلاغها بحكم أنها الجهة الحكومية المسئولة عن الأمن العام وسلاح الحدود والأمن الخاص وقوات المباحث	• وزارة الداخلية

الطرف ذي العلاقة	السبب	أمثلة
	والبحث الجنائي.	
مقدمو خدمات الإنترنت	من شأن إشعار مزودي خدمات الإنترنت (خاصة إذا كان مرسل الرسائل الاقتحامية (SPAM)عميل لنفس مزود خدمة الإنترنت) أن يساعد مقدمي خدمات الإنترنت على تحديد مشكلة الرسائل الاقتحامية (SPAM)على شبكاتهم ومن ثم اتخاذ القرارات المتعلقة بكيفية منع وصول مثل هذه الرسائل أخرى.	• أول نت • أثير • سعودي نت
مجلس التعاون لدول الخليج العربي.	يُعتبر التعاون على المستوى الدولي والإقليمي أساسياً لمكافحة الرسائل الاقتحامية، وبإمكان دول مجلس التعاون لدول الخليج العربي أن تعمل على التنسيق والتكامل الناجح بين دول المجلس في مجالات اهتماماتها المشتركة مثل المجالات القانونية والصناعية والتقنية.	• لم تُحدد بعد
الجهات الإحصائية	الجهات المسئولة عن عمل الإحصائيات تعتبر من الجماعات ذات العلاقة وذلك لأن الإبلاغ عن حالات الرسائل الاقتحامية (SPAM)سوف يساعدها على تجميع الإحصائيات المفيدة في وضع السياسات الأمنية والإجراءات المضادة للرسائل الاقتحامية مستقبلاً.	• MessageLabs • مزودو الحلول الأمنية، مثل سيمانتيك. • مقدمو خدمات البريد الإلكتروني.
المؤسسات الدولية	قد يقتضي الأمر إبلاغ جهة دولية ذات علاقة في حال أن منشأ الرسائل الاقتحامية (SPAM)كان مصدراً خارج المملكة العربية السعودية.	• فريق عمل مكافحة الاحتيال والتزييف (APWG) • فريق عمل مكافحة الاستخدام غير اللائق للرسائل (MAAWG) • سبام هاوس SPAMHAUS

٤-٦ تنفيذ العقوبة من الجماعات ذات العلاقة

عند تقديم التقرير بشأن الرسائل الاقتحامية، وتبين إدانة مرسل تلك الرسائل الاقتحامية (SPAM)ومسئوليته عنها، يتم توقيع العقوبة المحددة في النظام على ذلك المرسل من قبل الطرف ذي العلاقة المسئول عن تنفيذ أنظمة مكافحة الرسائل الاقتحامية.

وقد تختلف الجهة المنفذة للعقوبة، ويتوقف ذلك على مدى خطورة ونوع الرسائل الاقتحامية (SPAM)المرسلة، وبالتالي فهذه الجهات تشمل المحاكم و/أو الوزارات ذات العلاقة. في المرحلة الراهنة، لم يتم رسمياً بعد تحديد مسئولية تطبيق لوائح مكافحة الرسائل الاقتحامية (SPAM)على الرغم من أن بعض الأطراف ذات العلاقة المدرجة في الجدول أدناه قد تشارك في ذلك.

اسم الطرف ذي العلاقة	السبب	أمثلة
المحاكم	تنظر المحاكم في القضايا ذات الصلة بالرسائل الاقتحامية (SPAM)وتبت فيها بموجب القوانين المرعية في المملكة العربية السعودية.	• مجلس الشورى • ديوان المظالم • المحاكم الشرعية
الشرطة	تقوم الشرطة بناءً على تعليمات من المحاكم أو حسب تقديرها (في حال اعتبرت الاعتداء جنائياً) باتخاذ إجراء ضد المعتدين.	• الشرطة
الجهات الحكومية	تتولى وزارة التجارة (MOC) مسئولية الأنظمة واللوائح المنظمة لأعمال التسويق بالشركات، وبما أن الانتهاكات الصادرة من الرسائل الاقتحامية (SPAM)قد تقع ضمن نطاق قوانين حماية المستهلك المرعية في المملكة العربية السعودية، فإن وزارة التجارة (MOC) قد تشارك في آليات تنفيذ أنظمة مكافحة الرسائل الاقتحامية.	• وزارة التجارة
	تقع على عاتق وزارة الداخلية (MOI) مسئولية حفظ النظام في المملكة العربية السعودية، وتتبع الجهات الرئيسية المسئولة عن تنفيذ النظام في المملكة لوزارة الداخلية (MOI).	• وزارة الداخلية
	وزارة الاتصالات وتقنية المعلومات (MCIT) هي الجهة المسئولة عن وضع مشاريع الأنظمة واللوائح المتعلقة بالاتصالات وتقنية المعلومات، وبصفة خاصة تقع على الوزارة مهمة تنفيذ نظام جرائم المعلوماتية، وبالتالي فإن أي انتهاك من الرسائل الاقتحامية (SPAM)يقع تحت طائلة هذا القانون يستلزم تدخل وزارة الاتصالات وتقنية المعلومات (MCIT) كطرف ذي علاقة بهذا الانتهاك.	• وزارة الاتصالات وتقنية المعلومات

٤-٧ الخاتمة

يشترك عدد من الأطراف ذات العلاقة في دورة حياة نشاط الرسائل الاقتحامية، ويلعب كل طرف دوراً مختلفاً عن الأطراف الأخرى ضمن إطار دورة حياة الرسائل الاقتحامية.

ولكي يتسنى أن يتسم هيكل سياسة مكافحة الرسائل الاقتحامية (SPAM)بالفاعلية المتوخاة، فمن الضروري أن يؤخذ بعين الاعتبار معظم، إن لم يكن كل، الجماعات ذات العلاقة.

٥- الردود الواردة من الجهات ذات العلاقة

تشمل القائمة أدناه أسماء الأطراف ذات العلاقة التي تم تضمينها في البحث (المسح المبني على استمارات استطلاع الرأي و/أو مقابلات) الذي قام به فريق إرنست ويونغ أثناء تقييم الحالة الراهنة للرسائل الاقتحامية في المملكة العربية السعودية:

- مؤسسة النقد العربي السعودي؛
- مقدمو خدمات المعلومات؛
- مقدمو خدمات الهاتف الجوال؛
- المرخصين بتقديم خدمات رسائل الجوال القصيرة الجماعية؛
- مقدمو الحلول؛
- مقدمو خدمات الإنترنت؛
- الشركات؛
- الجامعات؛
- وزارة الداخلية؛
- هيئة الاتصالات وتقنية المعلومات؛
- مدينة الملك عبد العزيز للعلوم والتقنية / وحدة خدمات الإنترنت.

٥-١ مؤسسة النقد العربية السعودي

٥-١-١ الخلفية

تتولى مؤسسة النقد العربي السعودي(SAMA)، وهي البنك المركزي السعودي، مهمة الإشراف على البنوك التجارية، وهي الجهة المسئولة عن وضع الأنظمة واللوائح البنكية. تقوم المؤسسة بإصدار العملات الوطنية، تعمل كمصرف لدى الحكومة، وتشرف على البنوك التجارية، وتدير احتياطي النقد الأجنبي للمملكة العربية السعودية، وهي المسئولة عن نظام مراقبة البنوك وتقدم القواعد الأمنية المتعلقة البنكية عبر الإنترنت.

٥-١-٢ أهمية هذا الطرف ذي العلاقة

تقدم مؤسسة النقد العربي السعودي(SAMA) الإرشادات والقواعد الخاصة بأمن العمليات البنكية عبر الإنترنت، وهي المسئولة عن نظام مراقبة البنوك. بالتالي، تقوم البنوك مبدئياً بتوجيه البلاغات عن هجمات التزوير والاحتيال إلى المؤسسة التي بدورها تحيلها كل على حدة إلى وزارة الداخلية (MOI) وهيئة الاتصالات وتقنية المعلومات (CITC) المسئولة عن حجب الوصول إلى هذه المواقع واتخاذ الإجراءات العقابية المطبقة بهذا الصدد.

٥-٢ مقدمو خدمات المعلومات

٥-٢-١ الخلفية

مقدمو خدمة المعلومات هم الأطراف ذوي العلاقة بالمعلومات الذين يقدمون الربط بالإنترنت ويعملون كبوابات إلكترونية (Gateway) لمزودي خدمات الإنترنت ولبعض المؤسسات بهدف ربطها بالإنترنت. تم الاتصال بثلاثة من مزودي خدمات المعطيات الذين يحملون حالياً تراخيص من هيئة الاتصالات وتقنية المعلومات (CITC):

- شركة الاتصالات المتكاملة
- شركة الاتصالات السعودية
- بيانات العلا.

٥-٢-٢ أهمية هذا الطرف ذي العلاقة

مزودو خدمات المعلومات الثلاثة المذكورون أعلاه يمثلون العمود الفقري لجميع مزودي خدمات الإنترنت في المملكة العربية السعودية. يقوم مقدمو خدمات الإنترنت بتوقيع عقود مع مزودي خدمات المعطيات بهدف توفير خدمة الربط بالإنترنت، وأي ضوابط محتملة مطبقة لدى مزودي خدمات المعلومات من شأنها أن تفضي إلى حظر وصول الرسائل الاقتحامية (SPAM)الواردة والصادرة.

٥-٣ مقدمو خدمة الجوال

٥-٣-١ الخلفية

تم الاتصال مع اثنين من مقدمي خدمة الجوال هما شركة الاتصالات السعودية وشركة موبايلي. فالأولى وهي شركة الاتصالات السعودية هي المزود الأول لخدمة الهاتف الجوال، وهي علاوة على خدمة الهاتف الجوال، تقدم خدمات الهاتف الثابت وخدمات المعطيات والإنترنت، علماً أن خدمات المعطيات تتضمن خدمات الفاكس والواب (WAP) وجوال نت بالإضافة إلى خدمات التجوال الدولي للمشتركين لدى الشركة.

أما الشركة الثانية المزودة لخدمة الهاتف الجوال، وهي شركة اتحاد اتصالات، واسمها التجاري موبايلي، فتتولى تقديم خدمات نظام الهاتف العالمي المتنقل (GSM) وخدمات الجيل الثالث من الاتصالات، مثل المكالمات الصوتية، الرسائل متعددة الوسائط، (MMS)، خدمات (LBS)، خدمات التجوال الدولي، وخدمات (GPRS) وخدمات التجوال (GPRS EDGE).

٥-٣-٢ أهمية هذا الطرف ذي العلاقة

حيث أنه بالإمكان استخدام رسائل الجوال القصيرة (SMS)/الرسائل المتعددة الوسائط للترويج للبضائع والخدمات، بالتالي بإمكان مقدمي خدمة الجوال أن يسهموا بدور هام كونهم يمثلون العمود الفقري للمرخصين بتقديم خدمات الرسائل القصيرة الجماعية في المملكة العربية السعودية، فإن بإمكانهم تصفية الرسائل الاقتحامية (SPAM)وإغلاق المنافذ أمام مرسلي تلك الرسائل.

٥-٤ المرخصون لإرسال الرسائل القصيرة الجماعية الاقتحامية

٥-٤-١ الخلفية

تتيح رخصة تقديم خدمة الرسائل القصيرة الجماعية للشركات إرسال رسائلهم الجماعية إلى المشتركين، علماً أن هيئة الاتصالات وتقنية المعلومات (CITC) قد أصدرت أكثر من ٩٠ رخصة لتقديم خدمة الرسائل القصيرة الجماعية في المملكة، ومنهم على سبيل المثال:

- باب كوم؛ BAB.Com
- تواصل؛
- الشركة السعودية للأبحاث والنشر؛
- شركة الخليج الأولى First Gulf؛
- فوداتل ؛
- إلكترونيك كونسبتس Electronic Concepts؛
- سكاي تليكوم Sky Telecom Co؛
- وآخرون غيرهم؛

تم إجراء مقابلات مع ثمانية مقدمي خدمة رسائل قصيرة، بينما أجاب ١٣ على استمارة استطلاع الرأي.

٥-٤-٢ أهمية الطرف ذي العلاقة

أصحاب رخص الرسائل القصيرة الجماعية مفوضون بإرسال رسائل نصية قصيرة جماعية بموجب الشروط الموضحة في الرخص الممنوحة لهم من قبل هيئة الاتصالات وتقنية المعلومات (CITC). وبعض هذه الرسائل قد تُعتبر رسائل اقتحامية، وبالتالي يجب تنظيم عمل المرخصين بتقديم خدمات الرسائل القصيرة الجماعية ووضع حدود مقبولة لأعمالهم.

٥-٥ مزودو الحلول

٥-٥-١ الخلفية

يسهم مزودو الحلول بدور هام في مكافحة الرسائل الاقتحامية، فهم يقدمون الحلول الفنية التي تعتبر في غاية الأهمية للحد من الرسائل الاقتحامية، وقد تم الالتقاء باثنين من مزودي خدمة الحلول، بينما تم الاتصال على آخرين عبر البريد الإلكتروني وعلى الهاتف، ومن ضمن هؤلاء:

- سيمانتيك: تقدم خدمة BrightMail 6 التي يمكن استخدامها كبوابة إلكترونية للبريد بالاقتران مع خوادم (Mail Gateways) البريد وعلى خوادم (Mail Gateways) البريد؛
- سوفوس Sohpos: تقدم البرمجيات الأمنية مثل برمجيات مكافحة الفيروسات (Viruses) وبرمجيات مكافحة برامج التجسس (anti-spyware) وبرمجيات مكافحة الرسائل الاقتحامية (SPAM)وضوابط النفاذ إلى أجهزة الكمبيوتر المركبة على ضمن الشبكة وخوادم (Mail Gateways) البريد الإلكتروني والبوابات الإلكترونية للشبكات الأخرى؛
- آي أس أس ISS: تقدم منتجات وخدمات أمنية لتوفير الحماية الأمنية المسبقة للشركات ضد التهديدات على الإنترنت.
- كليرسويفت Clear Swift: تقدم MIME Sweeper للبروتوكول SMTP 5.2 (الذي يمكن استخدامه كبوابة للبريد الإلكتروني)، وكذلك MIME Sweeper للمقاسم (الذي يمكن استخدامه كوصلات لـخوادم (Mail Gateways) البريد الداخلية التابعة لـ (Exchange Mail/MDAs).
- سيرف كونترول SurfControl: تقدم مرشحات البريد الإلكتروني ومنتجات MailControl التي يمكن استخدامها كبوابة بريد إلكترونية؛
- وآخرين؛

٥-٥-٢ أهمية الطرف ذي العلاقة

يقدم مزودو الحلول الأمنية أدوات تصفية الرسائل الاقتحامية (SPAM)ومواد التوعية من أجل تصفية الرسائل الاقتحامية (SPAM)قبل وصولها إلى المستخدم النهائي، وينبغي على أدوات تصفية الرسائل الاقتحامية (SPAM)مواكبة سرعة تطور الأساليب الجديدة لمرسلي الرسائل الاقتحامية (SPAM)عند استخدام تلك الرسائل كأدوات لإرسال الفيروسات (Viruses) وهجمات البرامج الخبيثة وهجمات التزوير والتصيد (Phishing).

٥-٦ مقدمو خدمة الإنترنت

٥-٦-١ الخلفية

يوفر مقدمو خدمات الإنترنت وصلات للشركات والأفراد والجهات الحكومية، وبالتالي فهم يعتبرون الناقل للاتصالات الإلكترونية وتحديداً البريد الإلكتروني. وقد تم إجراء مقابلات مع اثنين من مزودي خدمات الإنترنت، بينما شارك ١٥ مزود خدمة إنترنت في المسح. وقد منحت هيئة الاتصالات وتقنية المعلومات (CITC) العديد ون التراخيص لمزودي خدمات الإنترنت، ومنهم على سبيل المثال:

- نسمة؛
- زاجل؛

- ميدونت؛
- أول نت؛
- أس بي أس نت؛
- شبكة نت؛
- صحارى نت؛
- سعودي نت؛ و
- وآخرين.

٥-٦-٢ أهمية الطرف ذي العلاقة

يقدم مزودو خدمات الإنترنت البنية الأساسية التي من خلالها تعبر حركة الإنترنت، وبإمكان مزودي خدمة الإنترنت نشر المرشحات (Filters) التي تحد من الرسائل الاقتحامية، وبإمكانها إغلاق المصادر الرئيسية للرسائل الاقتحامية وذلك باستخدام قوائم سوداء/بيضاء. علاوة على ذلك، قد يلعب مقدمو خدمات الإنترنت دوراً في رفع مستوى المعرفة والتوعية المتعلقة بالرسائل الاقتحامية، وكذلك استقبال الشكاوى من ضحايا هذه الرسائل، واتخاذ الإجراءات النظامية بحق مرسلي الرسائل الاقتحامية.

٥-٧ الشركات

٥-٧-١ الخلفية

تتلقى معظم الشركات كميات هائلة من البريد الإلكتروني الخاص بالإعلانات عن المنتجات والخدمات، ونتيجة لذلك، فمن المرجح أن تقع الشركات فريسة للرسائل الاقتحامية بما فيها الفاكس. وقد شملت هذه الدراسة ست وثلاثين شركة وجرى عقد لقاءات مع اثنتين منها.

٥-٧-٢ أهمية الطرف ذي العلاقة

إن الشركات غالباً ما تقع ضحية للرسائل الاقتحامية بحكم استخدامها المكثف للبريد الإلكتروني مما يجعلها أكثر عرضة للمزيد من التهديدات الناجمة عن الرسائل الاقتحامية. ومن ناحية أخرى، يمكن استغلال شبكات الشركات أيضاً لإرسال رسائل اقتحامية، وبالتالي يعتبر وجود مرشحات (Filters) وسياسات وبرامج توعية لدى تلك الشركات في غاية الأهمية للتقليل من كمية الرسائل الاقتحامية (SPAM)التي يتم إرسالها واستقبالها.

٥-٨ الجامعات

٥-٨-١ الخلفية

بعض الجامعات في المملكة العربية السعودية مثل جامعة الملك فهد للبترول والمعادن (KFUPM) وجامعة الملك سعود (KSU) وجامعة الملك فيصل (KFU) وغيرها من الجامعات الأخرى تعتمد اعتماداً كبيراً على الإنترنت والبريد الإلكتروني كوسيلة للاتصال والتواصل بين الإدارات والأساتذة والطلاب، وقد شمل مسح هذه الدراسة مقابلة ومشاركة اثنتين من هذه الجامعات.

٥-٨-٢ أهمية الطرف ذي العلاقة

تُعتبر شبكات الجامعات بصفة عامة معرضة للمتطفلين الذين يستخدمون أجهزة الجامعات كشبكات Botnets، وهكذا تصبح الحاسبات الآلية بالجامعات فريسة يجدها مرسلو الرسائل الاقتحامية (SPAM)جاذبة لشن هجماتهم.

٥-٩ وزارة الداخلية

٥-٩-١ الخلفية

وزارة الداخلية (MOI) هي المسئولة عن نظام مكافحة جرائم المعلوماتية الذي يهدف إلى وضع معايير قانونية وتنظيمية لمكافحة جرائم المعلومات والحاسب الآلي والإنترنت من خلال تحديد الجرائم ذات الصلة واتخاذ إجراءات تأديبية مقابل كل جريمة أو انتهاك.

٥-٩-٢ أهمية الطرف ذي العلاقة

بما أن وزارة الداخلية (MOI) هي المالك لنظام مكافحة جرائم المعلوماتية، فهي بالتالي تلعب دوراً هاماً في مكافحة الرسائل الاقتحامية، وقد أنشأت الوزارة مؤخراً وحدة جديدة تتولى المسئولية عن التحقيق في الجرائم الإلكترونية. وفي هذا الصدد، يعتبر التعاون بين وزارة الداخلية (MOI) وهيئة الاتصالات وتقنية المعلومات (CITC) ومؤسسة النقد العربي السعودي(SAMA)ة والأطراف الأخرى ذات العلاقة في غاية الأهمية لكي يتسنى مكافحة الرسائل الاقتحامية (SPAM)بالفعالية والكفاءة اللازمة.

٥-١٠ هيئة الاتصالات وتقنية المعلومات

٥-١٠-١ الخلفية

هيئة الاتصالات وتقنية المعلومات (CITC) هي الهيئة المنظمة لقطاع الاتصالات في المملكة العربية السعودية، وتتمتع الهيئة بشخصية اعتبارية واستقلال مالي بما يمكّنها من تحقيق أهدافها المنصوص عليها في نظام الاتصالات ولائحته التنفيذية ونظام هيئة الاتصالات وتقنية المعلومات (CITC). هيئة الاتصالات وتقنية المعلومات (CITC) مكلفة بحماية مصالح المستخدمين فيما يتعلق بخدمات الاتصالات العامة وخدمات الإنترنت، وهي التي تقترح اللوائح والأنظمة ذات العلاقة بقطاعات الاتصالات.

٥-١٠-٢ أهمية الطرف ذي العلاقة

تتولى هيئة الاتصالات وتقنية المعلومات (CITC) مهمة إدارة قطاع الاتصالات بالكامل في المملكة العربية السعودية. وعلى هذا الأساس، تخضع كافة محتويات الإنترنت التي تُشاهد داخل المملكة إلى تصفية مكثفة بهدف التحقق من المحتويات التي تتنافى مع القيم الوطنية والأنظمة المعمول بها في المملكة العربية السعودية، ويُحظر حظراً تاماً الوصول إلى المواقع المخلة بالآداب ومواقع الميسر والمخدرات، وتخضع هذه المواقع بصفة دائمة إلى التصفية من قبل هيئة الاتصالات وتقنية المعلومات (CITC). وبصفتها الجهة المنظمة لقطاع الاتصالات في المملكة، فإن هيئة الاتصالات وتقنية المعلومات (CITC) تتلقى الشكاوى الصادرة إليها من مؤسسة النقد العربي السعودي(SAMA) والشركات التجارية. وكجزء من مشروع المركز الوطني الإرشادي لتقنية المعلومات، فستقوم الهيئة بمراقبة الإنترنت في المملكة العربية السعودية وذلك لضمان حصول مستخدمي الإنترنت على إشعارات مبكرة في حالة وجود تهديد أمني، وبالتالي يمكن للهيئة أن تسهم بدور فعال في مكافحة الرسائل الاقتحامية.

٥-١١ مدينة الملك عبدالعزيز للعلوم والتقنية / وحدة خدمات الإنترنت

٥-١١-١ الخلفية

مدينة الملك عبد العزيز للعلوم والتقنية هي مؤسسة علمية تابعة لحكومة المملكة العربية السعودية تأسست عام ١٩٧٧م باسم المركز الوطني العربي السعودي للعلوم والتقنية، وفي عام ١٩٨٥م أُعيدت تسميتها إلى مدينة الملك عبد العزيز للعلوم والتقنية. وحدة خدمات الإنترنت هي إدارة تابعة لمدينة الملك عبد العزيز للعلوم والتقنية، ومسئولة عن خدمة الإنترنت في المملكة العربية السعودية وتقوم حالياً بتوفير خدمة الإنترنت للمؤسسات الأكاديمية والبحثية.

٥-١١-٢ أهمية الطرف ذي العلاقة

تتولى مدينة الملك عبد العزيز للعلوم والتقنية المهمة المكلفة بها في تطوير العلوم والتقنية في المملكة العربية السعودية وذلك من خلال التنسيق والتعاون مع مختلف الجامعات والهيئات والمؤسسات المختصة بالأبحاث والتقنية، وكذلك تتولى

تشجيع الخبراء السعوديين على اختيار الأبحاث التي تساعد على تطوير وتنمية المجتمع. كانت مدينة الملك عبد العزيز للعلوم والتقنية مكلفة بتنظيم الإنترنت والإشراف عليه قبل انتقاله إلى هيئة الاتصالات وتقنية المعلومات (CITC)، وتعمل المدينة في الوقت الراهن كمزود لخدمات الإنترنت الأكاديمية، وهي بالتالي مسئولة عن توفير خدمات الإنترنت القياسية والحديثة والمختبرات والتقنيات ذات الصلة للجامعات ومراكز البحوث والوكالات والهيئات والمؤسسات السعودية.

٥-١٢ الاهتمامات الرئيسية للأطراف ذات العلاقة وتوصياتها

تم إجراء مقابلات مع الأطراف ذات العلاقة التي حددتها الدراسة وذلك باستخدام استبيانات (استمارات استطلاع راي) مدروسة ومبرمجة، وكان هدف الدراسة من تلك الاستبيانات والاستطلاعات يتمثل في الحصول على استجابة من الجهات المستهدفة حول آرائها ووجهات نظرها واهتماماتها بالوضع الراهن المتعلق بالرسائل الاقتحامية (SPAM)في المملكة العربية السعودية.

يحتوي هذا الجزء على الاهتمامات والتوصيات الرئيسية المقدمة من مختلف الأطراف ذات العلاقة حول الرسائل الاقتحامية.

وقد أفادت جميع الأطراف ذات العلاقة بعدم وجود قوانين في الوقت الراهن في المملكة العربية السعودية تحدد تشريعات للرسائل الاقتحامية على الرغم من وجود بعض الأحكام ذات الصلة بالرسائل الاقتحامية (SPAM)ضمن عدد من الأنظمة المختلفة وكذلك متطلبات/ اتفاقيات إصدار تراخيص مقدمي الخدمات ذات الصلة. ولهذا السبب، لا توجد أنظمة مختصة بتجميع واستخدام وتبادل وبيع تفاصيل الاتصالات الشخصية مثل عناوين البريد الإلكتروني وأرقام الهواتف. كما أشارت بعض الأطراف ذات العلاقة إلى عدم وجود تعاون بين مختلف الهيئات في مكافحة الرسائل الاقتحامية. فعلى سبيل المثال، قامت مؤسسة النقد العربي السعودي(SAMA) ووزارة الداخلية (MOI) وهيئة الاتصالات وتقنية المعلومات (CITC) بوضع إجراء غير رسمي للتعاون فيما بينها بخصوص القضايا ذات الصلة الرسائل الاقتحامية/ التزوير والاحتيال. غير أنه على الرغم من ذلك، فإنه لم يتم وضع إجراء رسمي للتعامل مع الشكاوى وتحويلها إلى السلطات المختصة. كما أثير عدم وجود لائحة ضوابط سلوكية لمزودي خدمات الإنترنت أو المتعاملين بالتسويق الإلكتروني في المملكة العربية السعودية.

إن رسائل البريد الإلكتروني الاقتحامية، علاوة على ما تسببه من إزعاج ومضايقة، تثير مشاكل تتعلق بسعات الأنظمة وعرض النطاق وأداء العاملين، فأثناء الاجتماعات التي عُقدت مع مختلف الأطراف ذات العلاقة، أثار كثير منهم عدداً من النقاط، بينما اقترح آخرون بعض الضوابط الفنية.

وقد اقترحت بعض الأطراف وجوب قيام هيئة الاتصالات وتقنية المعلومات (CITC) بتأمين مزودين لاستضافة البريد الإلكتروني التجاري الآمن تتمثل مهمتهم في استلام رسائل البريد الإلكتروني نيابة عن الشركات ومن ثم تصفيتها وتنقيتها قبل تسليمها لخوادم (Mail Gateways) بريد الشركات.

مقدمو خدمات الإنترنت

أثار مقدمو خدمات الإنترنت موضوع النقص في الكوادر المؤهلة فنياً، وأشاروا إلى أنهم تعوزهم الكوادر الفنية الكافية وأنهم لهذا السبب عاجزين عن المعالجة الفعالة لمشكلة الرسائل الاقتحامية. كما أوضح مقدمو خدمات الإنترنت إلى أنهم يقومون بتركيب الأدوات/المرشحات (Filters) لغرض توفير الحماية لصناديق بريد العملاء الذين يقررون استخدام خوادم (Mail Gateways) البريد الإلكتروني التابعة لمزودي خدمات الإنترنت. بالتالي، يتضح أن مزودي خدمات الإنترنت لا يعملون على تصفية كل حركة الرسائل المتدفقة عبر شبكاتهم بسبب القصور الراهن في ميزانياتهم ومواردهم وقدراتهم. لكن مع ذلك، تشير إحدى النتائج إلى أن مزودي الخدمات الذين قاموا بنشر قوائم سوداء على الموجهات (Routers) أو البوابات الإلكترونية التي لديهم، أفادوا بانخفاض معدلات الرسائل الاقتحامية (SPAM)لديهم، وكذلك لدى العملاء.

مقدمو خدمات البيانات:

أثار مقدمو خدمات البيانات موضوع النقص في الكوادر المؤهلة فنياً وأشاروا إلى أنهم تعوزهم الكوادر الفنية الكافية وأنهم لهذا السبب عاجزين عن المعالجة الفعالة لقضية الرسائل الاقتحامية، كما أوضح مقدمو خدمات المعطيات أنهم لا تتوفر لديهم ضوابط حالياً تتعلق برسائل البريد الإلكتروني الاقتحامية، وأنهم يوصون بشدة بتركيب مرشحات (Filters) مركزية للرسائل الاقتحامية على مستوى مزودي خدمات الإنترنت وأقل من ذلك، لأن هذه المرشحات (Filters) من شأنها أن تقلل من جودة الخدمات المقدمة من مزودي خدمات البيانات إذا ركبت على أنظمتهم الأساسية. غير أن مقدمي خدمة البيانات يوافقون على إمكانية نشر القوائم السوداء على الموجهات (Routers) التي لديهم لضمان عدم قيام مرسلي الرسائل الاقتحامية (SPAM)المعروفين بإرسال رسائل بريد إلكتروني إلى المستخدمين في المملكة العربية السعودية، بيد أنهم

أكدوا أن هذه القوائم السوداء يتعين أن تكون دقيقة جداً، إذا أنها قد تؤدي إلى إغلاق مسار الحركة الشرعية للبريد الإلكتروني.

مقدمو خدمة الجوال:

اقترح مقدمو خدمة الجوال أن تركز أنظمة الرسائل القصيرة الاقتحامية على تراخيص مزودي خدمة الرسائل القصيرة الجماعية واستبعاد الإعلانات. كما اقترحوا بوجوب مراقبة وضبط سجلات المواقع الإلكترونية كعنصر مكمل لتحديد المسئوليات ولمراقبة المواقع الإلكترونية المرسلة للرسائل القصيرة الاقتحامية.

يتلقى مقدمو خدمة الجوال يومياً أعداداً هائلة من الرسائل القصيرة بالجوال التي منشأها مصادر خارج المملكة العربية السعودية، علماً أن بعض هذه الرسائل هي رسائل اقتحامية. رغم أن الأنظمة الحالية المتوفرة لدى مقدمي خدمة الجوال لا تحتوي على مرشحات (Filters) متطورة لتحديد الرسائل القصيرة الاقتحامية، إلا أن مقدمي خدمة الجوال قد وضعوا ضوابط لضمان فحص وحجب الرسائل القصيرة الجماعية الدولية إذا أعتبرت رسائل اقتحامية. بالإضافة إلى ذلك، يعمل مقدمو خدمة الجوال على تطوير أنظمتهم لضمان تطبيقها الدقيق لضوابط مكافحة الرسائل الاقتحامية. وفي هذا الشأن، ذكرت شركة موبايلي أن ١,٧% من الرسائل القصيرة الحالية هي رسائل اقتحامية.

مقدمو خدمة الرسائل النصية القصيرة الجماعية:

اقترح مقدمو خدمة الرسائل النصية القصيرة الجماعية وضع وتطبيق نظام لمكافحة الرسائل الاقتحامية (SPAM)على أن يتضمن هذا النظام عقوبات صارمة كأفضل وسيلة لضبط الرسائل الاقتحامية (SPAM)عبر الرسائل القصيرة. علاوة على ذلك، ومن أجل التعرف على مقدمي خدمة الرسائل القصيرة الجماعية الذين هم مصدر هذه الرسائل، فقد اقترحت الشركات المقدمة لخدمة الرسائل القصيرة الجماعية تحقيق ذلك الهدف من خلال تتبع الأرقام الأساسية (Premium numbers) المضمنة في هذه الرسائل، على أن تتم عملية المتابعة بالتنسيق مع شركة الاتصالات السعودية وشركة موبايلي.

مؤسسة النقد العربي السعودي:

طرحت مؤسسة النقد العربي السعودي(SAMA) العديد من المبادرات الهادفة إلى مكافحة الاحتيال والتزوير سواءً كان ذلك من خلال تشجيع البنوك على الانضمام للمؤسسات الدولية لمكافحة التزوير والاحتيال أو من خلال تنسيق الجهود مع هيئة الاتصالات وتقنية المعلومات (CITC) لحجب الوصول إلى المواقع الإلكترونية التي تعتبر مصادراً للتزوير و التصيد (Phishing). كما تقوم المؤسسة بمتابعات منتظمة مع البنوك التي كانت عرضة لهجمات التزوير والاحتيال، وذلك بعد إغلاق مواقع التزوير والاحتيال على الشبكة بغية تقييم أي أضرار محتملة قد تلحق بتك البنوك نتيجة لتلك الهجمات. كما ذكرت المؤسسة أن لديها إجراءات صارمة يتعين تطبيقها من قبل البنوك العاملة بترخيص من المؤسسة وبموجب نظام مراقبة البنوك. وتجري مؤسسة النقد العربي السعودي(SAMA)ة مراجعات منتظمة لضمان تقيد المؤسسات المالية بأنظمة ولوائح المؤسسة.

علاوة على ما ورد أعلاه، قامت مؤسسة النقد العربي السعودي(SAMA) بتوزيع إرشادات أمنية على البنوك في موقعها الإلكتروني www.sama.gov.sa ، وقد وردت إلى المؤسسة ٧٢ حالة من هجمات الاحتيال والتزوير على البنوك السعودية خلال العام المنصرم.

بالإضافة إلى ذلك، ذكرت المؤسسة أن التعاون القائم حالياً في تنفيذ النظام ليس بمستوى كفاءة التنسيق الذي يتعين أن يكون قائماً بين المؤسسة من جهة ووزارة الداخلية (MOI) وهيئة الاتصالات وتقنية المعلومات (CITC) من جهة أخرى بغية إصدار أمر لحجب مواقع التزوير والاحتيال من خلال هيئة الاتصالات وتقنية المعلومات (CITC)، ويرجع السبب في ذلك إلى أن البيروقراطية تتسبب أحياناً في تأخير خطير قبل اتخاذ أي إجراء ضد المعتدين.

وزارة الداخلية:

اقترحت وزارة الداخلية (MOI) أن يتم الاتصال بهدف الإبلاغ عن حالات الرسائل الاقتحامية (SPAM)مع هيئة الاتصالات وتقنية المعلومات (CITC) أو مع وحدة مكافحة الجرائم الإلكترونية التي تأسست مؤخراً، ويمكن بعد ذلك إحالة الحالة إلى مكتب التحقيق والإدعاء العام الذي قد يستعين بمهارات فنية من أطراف أخرى بما فيها هيئة الاتصالات وتقنية المعلومات (CITC).

الجامعات:

تقر الجامعات بأن شبكاتها وأجهزتها جاذبة لمرسلي الرسائل الاقتحامية (SPAM)وذلك لأن بالإمكان تحويلها إلى حاضنات للرسائل الاقتحامية Zombies[2]. لهذا السبب، قامت الجامعات بنشر ضوابط أمنية مختلفة للتخفيف من قضايا الرسائل الاقتحامية، هذا علماً أن بعض الجامعات لا تسمح للطلاب باستخدام الحاسبات الآلية المحمولة للدخول إلى الإنترنت باستخدام شبكات الجامعة بسبب النقص في الموارد المتاحة لديها. فضلاً عن أنه عند السماح بوصول الطلاب إلى الإنترنت، فإن تهديدات الرسائل الاقتحامية (SPAM)قد تتزايد وبالتالي قد يتطلب الأمر ضوابط أمنية إضافية. وقد اقترحت الجامعات وضع نظام لمكافحة الجرائم الإلكترونية (Cybercrime) يتضمن مكافحة الرسائل الاقتحامية. كما اقترحت الجامعات أهمية وضع برنامج لنشر الوعي بهدف تثقيف الناس بمخاطر الرسائل الاقتحامية.

مدينة الملك عبد العزيز للعلوم والتقنية ـ وحدة خدمات الإنترنت:

أشارت وحدة خدمات الإنترنت بأنها لا تقوم في الوقت الراهن بتصفية عرض النطاق المقدم إلى الجامعات بهدف تنظيفه من الرسائل الاقتحامية، لكن الوحدة قد تأخذ في الاعتبار تقديم عرض نطاق مصفى إلى الجامعات خاصة وأن الجامعات لا تتوفر لديها الموارد الفنية المطلوبة لنشر هذه الحلول المعقدة فنياً.

أكدت وحدة خدمات الإنترنت بمدينة الملك عبد العزيز للعلوم والتقنية على أهمية توقيع اتفاقيات مع دول أخرى ومع هيئات إنفاذ الأنظمة الدولية القائمة حالياً، كما اقترحت الوحدة إقامة تعاون مع الهيئات الإقليمية في دول مجلس التعاون لدول الخليج العربي وأن تكون آلية البلاغات واضحة ومباشرة، بينما يتعين أن يكون التطبيق مبسطاً جداً وأن يؤخذ التعاون الدولي في غاية الأهمية من أجل تحقيق هذا الهدف.

الشركات:

معظم الشركات تستخدم برمجيات مكافحة الرسائل الاقتحامية (SPAM)لتنقية بريدها الإلكتروني من الرسائل الاقتحامية، وعلى الرغم من أن بعض الشركات لديها قواعد بيانات ضخمة إلا أنها لم تكثف جهودها لحماية سرية هذه المعلومات وبالتالي منع مرسلي الرسائل الاقتحامية (SPAM)من التطفل على هذه المعلومات، ويُعزى السبب في ذلك إلى أن حماية هذه المعلومات لا تخضع لنظام لديه آلية تنفيذية.

من ناحية أخرى، الشركات التي تتعرض لاعتداءات الرسائل الاقتحامية (SPAM)لم تطور برامج لتوعية المستخدمين بكيفية استخدام الإنترنت مع التقليل من عدد الجهات التي لها علم بعناوين بريدها الإلكتروني بهدف تقليص احتمال اكتشاف مرسلي الرسائل الاقتحامية (SPAM)لعناوين بريدها الإلكتروني.

البنوك:

تقترح البنوك تطبيق تدابير مراقبة وإجراءات تبليغ واضحة في حال كان مصدر الرسالة الاقتحامية من مزود خدمة إنترنت محلي. وبالإضافة إلى ذلك، يتم حالياً وضع إجراء رسمي للتبليغ عن شكاوى التزوير و التصيد (Phishing) التي لها علاقة بالبنوك مثل تعليم المستخدمين وإرشادات التوعية.

---

[2] الكمبيوتر الحاضن (Zombie) هو كمبيوتر موصول بالإنترنت تمت السيطرة عليه بواسطة برنامج لفك الشفرة الأمنية أو فيروس كمبيوتر أو أحصنة طروادة، ومعظم أصحاب هذه الأجهزة لا يدركون أن أجهزتهم مستخدمة على هذه الهيئة، وتستخدم هذه الأجهزة لإرسال الرسائل الاقتحامية.

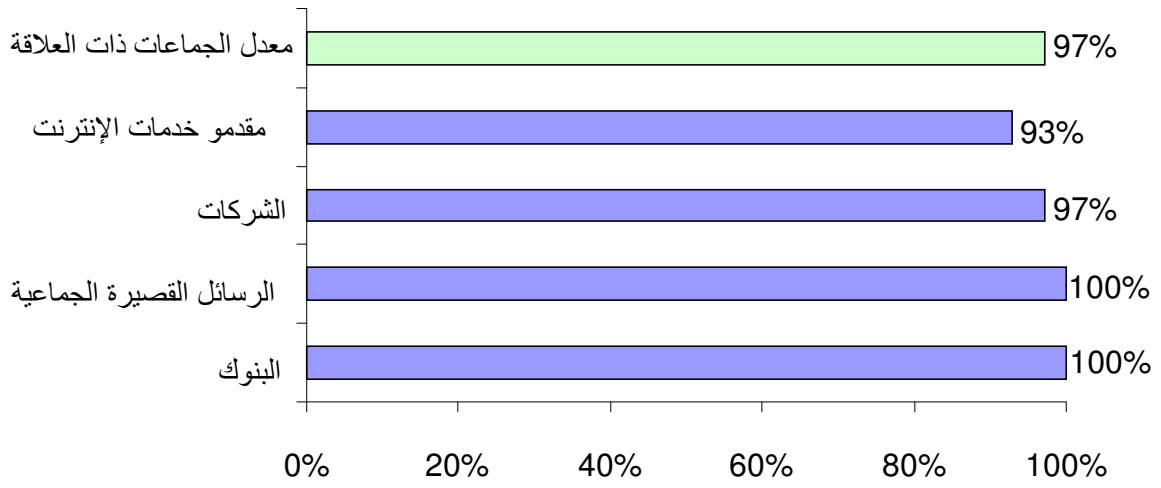
٦ نتائج المسح باستخدام استمارات استطلاع الرأي

يوضح هذا القسم النتائج التي توصلنا إليها باستخدام الإحصائيات المقدمة من قبل الجماعات ذات العلاقة من خلال إجاباتهم على الأسئلة المطروحة في استمارات استطلاع الرأي، وقد تم تقسيم النتائج إلى ثلاث فئات:

- تعريف الرسائل الاقتحامية،
- حجم المشكلة،
- والأسلوب المتبع حالياً من جانب الأطراف ذات العلاقة لمعالجة الرسائل الاقتحامية.

٦-١ تعريف الرسائل الاقتحامية

مثلما هو موضح في الشكل-١ أدناه، تتفق معظم الأطراف ذات العلاقة في المملكة العربية السعودية على تعريف الرسائل الاقتحامية (SPAM)الذي اقترحناه في استمارة استطلاع الرأي، ونص ذلك التعريف للرسائل الاقتحامية على ما يلي: رسائل واتصالات جماعية[3] غير مطلوبة[4] تحمل محتويات تجارية أو مسيئة أو مرفوضة يتم إرسالها بالجملة (بشكل جماعي) إلى مجموعة من الناس أو الأفراد دون موافقتهم، ويتم الإرسال بواسطة البريد الإلكتروني أو أجهزة الفاكس أو الرسائل الفورية مثل رسائل الجوال القصيرة (SMS).



الشكل (١): الاتفاق على تعريف الرسائل الاقتحامية (SPAM)

٦-٢ حجم المشكلة

يصف هذا القسم من التقرير حجم مشكلة الرسائل الاقتحامية (SPAM)في المملكة العربية السعودية.

فباستخدام البيانات المقدمة من قبل مجموعة من مقدمي خدمات الإنترنت الذين ساندوا هذا المشروع، تم تحديد معدل رسائل البريد الإلكتروني الاقتحامية في المملكة بنسبة ٥١%[5]. وقد تم تجاهل الإحصائيات المجمعة من المصادر الأخرى مثل الشركات، وذلك على اعتبار ما يلي:

---

[3] الرسائل الإلكترونية المرسلة دوت الموافقة الصريحة أو الضمنية للمستلم، وهي ذات طابع إعلاني أو ترويجي.

[4] الرسائل المرسلة بأعداد تفوق حداً معيناً مسبق التحديد ضمن فترة زمنية مسبقة التحديد.

[5] الرسائل التي ترسل بأعداد تتجاوز حداً معيناً مسبق التحديد خلال فترة زمنية محددة مسبقاً.

- بعض الشركات قدمت مجرد تقديرات في الوقت الذي لا تتوفر لديها أدوات تقارير يمكن أن تقدم هذه المعلومات مباشرة.
- شركات أخرى قدمت إحصائياتها، بيد أن معدلات الرسائل الاقتحامية (SPAM)لديها كانت متدنية نظراً لأن بعض مزودي خدمة الإنترنت يوزعون فعلاً قوائم سوداء في بواباتها الإلكترونية، وبالتالي يتم حجب كمية كبيرة من الرسائل الاقتحامية (SPAM)قبل أن تصل إلى هذه الشركات.

الأرقام المأخوذة من بائعي منتجات مكافحة الرسائل الاقتحامية، مثل (Message Labs) و (Symantec) تبدو قريبة جداً من الأرقام المأخوذة من مجموعة مقدمي خدمات الإنترنت. وقد أفادت Message Labs[6] بأن معدل الرسائل الاقتحامية (SPAM)في المملكة العربية السعودية للعام ٢٠٠٦م كان بحدود[٣] ٤٨,٣%[٧]، بينما أفادت Symantec[٨] أن معدل الرسائل الاقتحامية (SPAM)للعام ٢٠٠٦م كان بحدود ٥٩%. ومن ناحية أخرى، أفادت Message Labs[9] أن معدل الرسائل الاقتحامية (SPAM)(للعام ٢٠٠٧م حتى شهر يوليو) قد بلغ حوالي ٤٢,٧%.

أفادت شركة موبايلي أن معدل رسائل الجوال القصيرة (SMS) الاقتحامية في المملكة العربية السعودية بلغ ١,٧%، ويتعين ملاحظة أنه على الرغم من أن شركة موبايلي قد استخدمت تعريف النظام العالمي للهواتف المتنقلة GSMA للرسائل الاقتحامية[١٠] في تقريرها عن هذا الرقم، إلا أن الشركة لم تضمّن في هذا الرقم تلك الرسائل التجارية غير المطلوبة Unsolicited والتي هي رسائل تجارية في طبيعتها. بناءً على ذلك، هذا الرقم يتوافق مع الرسائل النصية القصيرة التي حوت محتويات جنسية ورسائل قصيرة تنطوي على خداع وغش باستخدام أرقام الفئة ٧٠٠.

فيما يتعلق بالرسائل القصيرة الاقتحامية، فقد أفاد مقدمو خدمة الجوال أن معدلها يبلغ ١,٧%. بالإضافة إلى ذلك، حيث أن ٦٥% من هذه الرسائل النصية القصيرة هي تجارية، ٢٠% بذيئة، ٢% سياسية، ٣% دينية، ٥% تتعلق بأسواق الأسهم و٥% ذات أغراض أخرى.

وبناءً على إفادات الأطراف ذات العلاقة التي شملها المسح، فإن رسائل البريد الإلكتروني الاقتحامية التي تم استلامها من قبلهم كان على أربعة أنواع حسبما هو موضح في الشكل-٢. وقد اعتبر (٦٤%) من المستجيبين للمسح أن رسائل التسويق المباشر كانت هي الأكثر شيوعاً من الرسائل الاقتحامية، بينما اعتبر ٢٥% منهم أن البريد الإلكتروني المتعلق بالجنس هو النوع الأكثر شيوعاً بين للرسائل الاقتحامية فيما اعتبر ٥% فقط أن الرسائل الاقتحامية (SPAM)الدينية تمثل نوعاً رئيسياً من الرسائل الاقتحامية. على ضوء ذلك، من المحتمل أن يؤدي ضبط ومراقبة الرسائل الاقتحامية (SPAM)التجارية إلى خفض كبير في كمية الرسائل الاقتحامية.

---

[6] شارك في المسح العديد من مقدمي خدمة الإنترنت على مدار ٨ شهور. وقد أخذنا في الاعتبار فقط الإحصاءات الشهرية التي زودنا خلالها مقدمو الخدمة بأرقام دقيقة. ويمثل هذا الرقم معدل الرسائل الاقتحامية على مدار تلك الشهور.

[7] البيانات المقدمة من (Message Labs) مبنية على إحصائيات وتحليلات على حزمة من مخاطر أمن البريد الإلكتروني في شتى أرجاء العالم. ويستند (Message Labs Intelligence) على مدخلات بيانات حية مأخوذة من شبكتهم العالمية من أبراج المراقبة والتي تحصي الملايين من الرسائل الإلكترونية يومياً.

[8] تم الحصول على هذا الرقم باستخراج معدل الرسائل الاقتحامية المتنوعة التي تم جمعها من خلال أجهزة استشعار مختلفة.

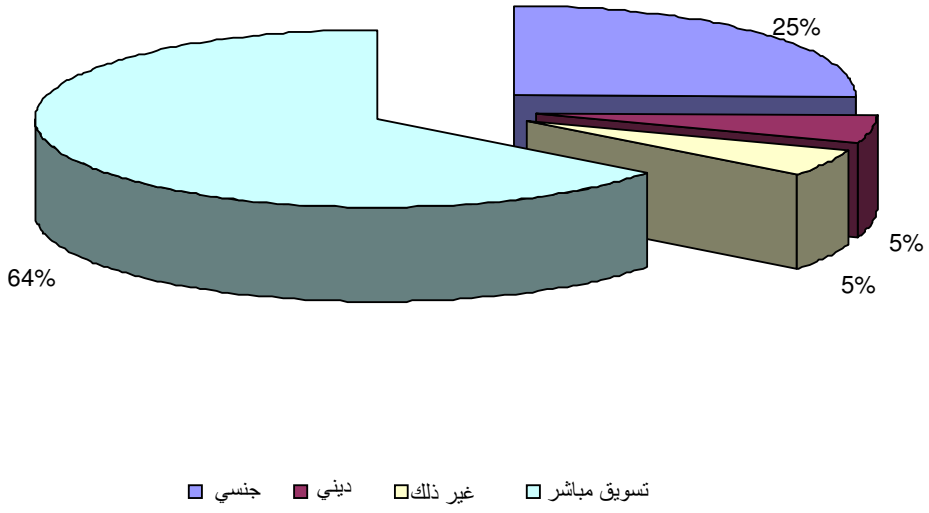
[9] البيانات الواردة في هذا التحليل تستند إلى الرسائل الاقتحامية التي رصدتها أجهزة استشعار شبكة سيمانتيك (Symantec Probe) المنتشرة في أكثر من ١٨٠ دولة

[10] قواعد العمل لدى (GSMA) توضح التزام مشغلي خدمات الاتصالات المتنقلة بمكافحة رسائل الجوال الاقتحامية والحد من أثرها على العملاء. وتنطبق قواعد العمل هذه على الاتصالات غير المطلوبة المرسلة عبر الرسائل القصيرة ورسائل الوسائط المتعددة (والتي يشار لها بعبارة رسائل الجوال الاقتحامية)، وتتضمن بشكل محدد ما يلي:

أ) الرسائل القصيرة التجارية أو الرسائل المتعددة الوسائط المرسلة للعملاء لتشجيعهم بصورة مباشرة أو غير مباشرة للاتصال أو إرسال رسائل قصيرة أو أية رسائل إلكترونية إلى أرقام ذات تكلفة اتصال عالية.

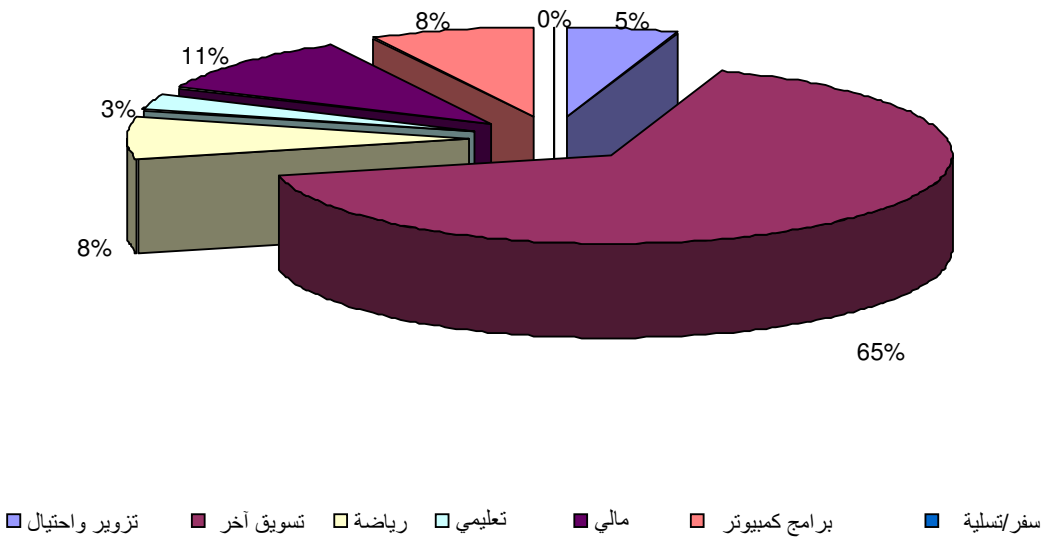
ب) الرسائل القصيرة أو الرسائل متعددة الوسائط المرسلة إلى عملاء بشكل جماعي بهدف الغش (مثل التزوير والخداع والتحايل).

ولأغراض قواعد ممارسة الأعمال، فإن الرسائل التجارية القصيرة أو الرسائل متعددة الوسائط التجارية تعني الرسائل القصيرة أو الرسائل متعددة الوسائط المصممة بصورة مباشرة أو غير مباشرة، لترويج الخدمات أو البضائع أو صورة أي شخص يقوم بنشاط تجاري أو يؤدي أية مهنة منظمة.



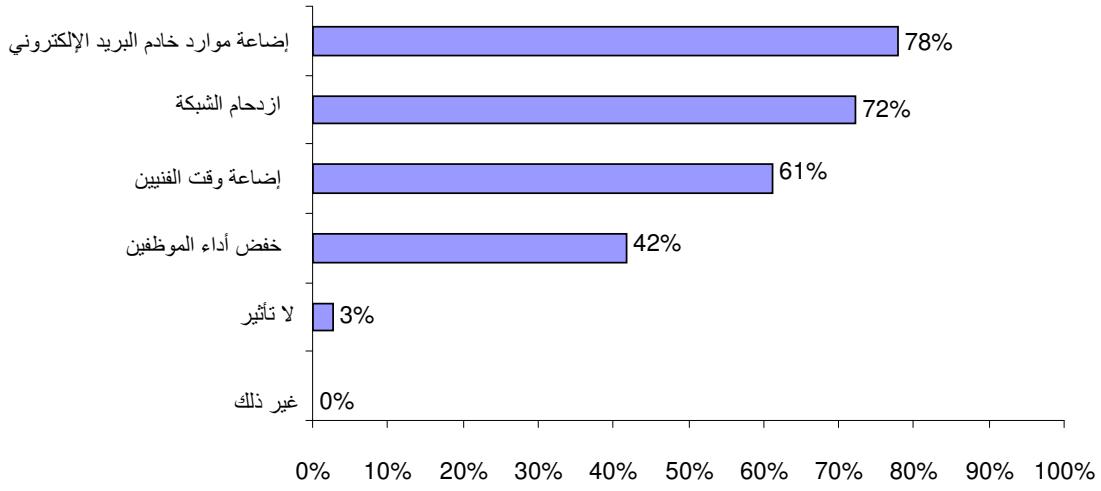
الشكل (٢): آراء الأطراف التي قامت بالرد حول أكثر أنوع الرسائل الاقتحامية (SPAM)شيوعاً

اعتبر المستجيبون للدراسة أن الرسائل ذات العلاقة بالتمويل (١١%) والرياضة (٨%) وبرمجيات الحاسب الآلي (٨%) هي الأنواع الأكثر هيمنة من بين الرسائل الاقتحامية (SPAM)التجارية. الأنواع الأخرى من الرسائل الاقتحامية (SPAM)كانت إما أن لها صلة بالتزوير والتصيد (Phishing) أو بالتعليم، فيما تم تصنيف جزء كبير من الرسائل الاقتحامية (SPAM)الواردة تحت مسمى "رسائل تسويق أخرى"، وقد أوضح المستجيبون للدراسة أنهم يشيرون من خلال عبارة "رسائل تسويق أخرى" إلى الرسائل التي تروج للمبيعات غير الشرعية للمنتجات (مثل الفياجرا).



الشكل (٣): تحليل آراء الأطراف التي قامت بالرد حول أنواع التسويق المباشر للرسائل الاقتحامية

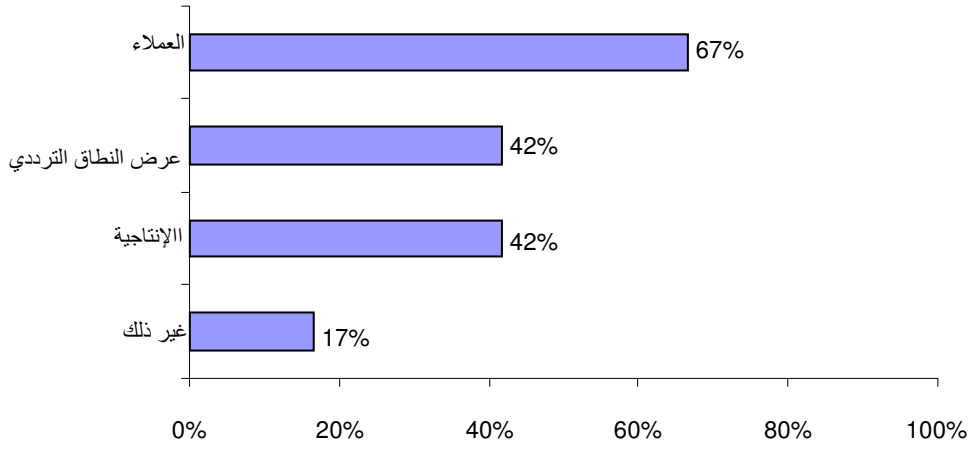
تعتقد ٧٨% من الشركات التي استجابت للمسح أن الأثر الأساسي للرسائل الاقتحامية كان منصباً على موارد خوادم (Mail Gateways) البريد الإلكتروني التابعة لها، بينما تعتقد ٧٢% أن الرسائل الاقتحامية (SPAM)أدت إلى ازدحام شبكاتها. الآثار الأخرى شملت الزمن الذي تهدره العمالة الفنية بهذه الشركات للتعامل مع الرسائل الاقتحامية (SPAM)(٦١% من المستجيبين)، ومما يثير الدهشة أن ٤٢% فقط من الشركات المستجيبة للمسح ذكرت أن الرسائل الاقتحامية (SPAM)قد أدت إلى تدني أداء العاملين لديها.



الشكل (٤): نسبة الشركات التي ترى أن الرسائل الاقتحامية (SPAM)تؤثر عليها بحسب المعايير الموضحة في الشكل

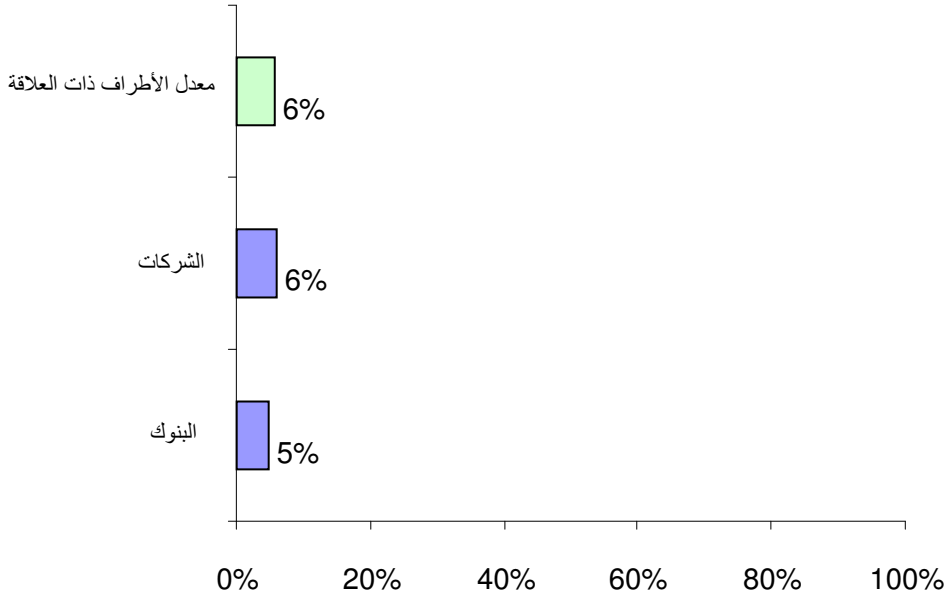
عندما طُرح السؤال على مقدمي خدمات الإنترنت لتحديد آثار الرسائل الاقتحامية (SPAM)على مؤسساتهم، كانت النتائج مثلما هو موضح في الشكل (٥). فقد رأى ٦٧% من مقدمي خدمات الإنترنت أن العملاء هم الأكثر تأثراً بالرسائل الاقتحامية، كما كان هناك أثر كبير على عرض النطاق والإنتاجية بنسبة بلغت ٤٢%. وأفاد المستجيبون

للدراسة أيضاً أن عرض النطاق المستهلك بواسطة الرسائل الاقتحامية (SPAM)تراوح ما بين ٥% إلى ٢٥% من إجمالي عرض النطاق المتوفر لديهم.

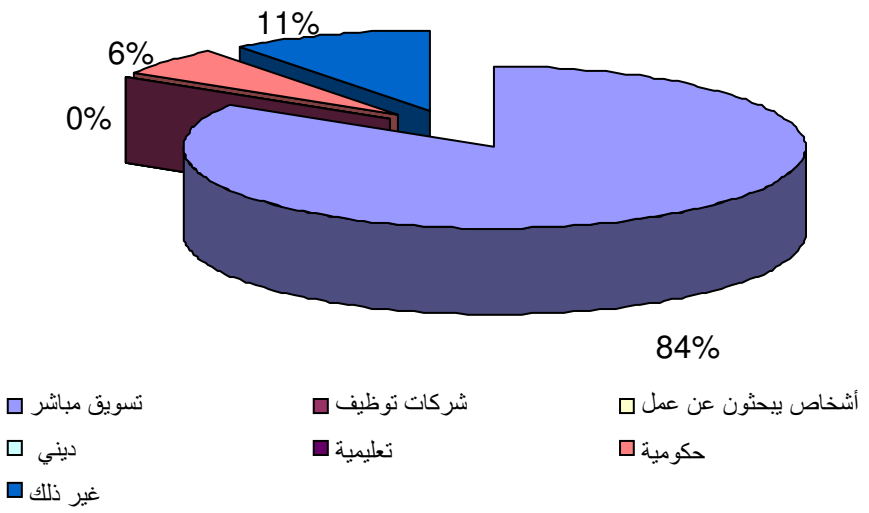


الشكل (٥): نسبة مقدمي خدمة الإنترنت التي يرون أن الرسائل الاقتحامية (SPAM)تؤثر عليهم بحسب المعايير الموضحة في الشكل

لم يعتبر أي من المستجيبين أن الرسائل الاقتحامية (SPAM)بالفاكس تمثل مصدراً كبيراً للرسائل الاقتحامية في المملكة العربية السعودية. يوضح الشكل (٦) كمية الفاكسات المستلمة التي تعتبر رسائل اقتحامية. وبحسب إفادة المستجيبين للدراسة، فإن الرسائل الاقتحامية (SPAM)بالفاكس لا تشكل قضية كبيرة في المملكة العربية السعودية، وأن معظم الرسائل الاقتحامية (SPAM)بالفاكس تميل لكونها ذات طابع تجاري، وقد أكد ٨٤% من المستجيبين أن الرسائل الاقتحامية (SPAM)التجارية كانت هي الشكل الأكثر شيوعاً من بين الرسائل الاقتحامية (SPAM)التي تم استلامها.

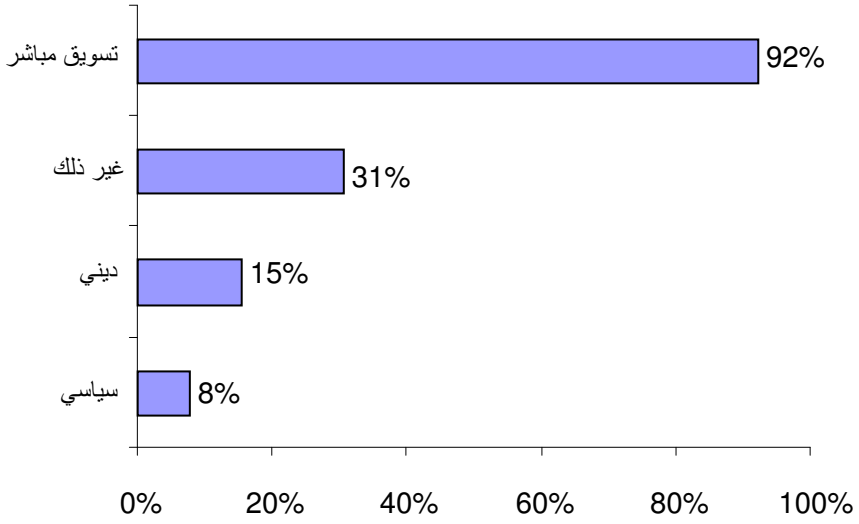


الشكل (٦): رسائل الفاكس الاقتحامية المستلمة



الشكل (1): أنواع رسائل الفاكس الاقتحامية المستلمة

يقدم مقدمو الرسائل القصيرة الجماعية ثلاثة أنواع من الخدمات: الترويج للمنتجات، الترويج للخدمات والإعلانات نيابة عن الآخرين. الرسائل المرسلة عن طريق وحدات مقدمي هذه الخدمات هي إما أن تكون تسويقية، أو دينية، أو سياسية مثلما هو موضح في الشكل (٨). يتضح جلياً أن الغالبية العظمى من المرخص لهم بتقديم خدمة الرسائل القصيرة الجماعية يرسلون رسائل للتسويق المباشر.



الشكل (٨): نسبة الأطراف المرخصة بإرسال الرسائل القصيرة الاقتحامية الجماعية بحسب المعايير الموضحة في الشكل [11]

[11] وفقاً لإفادة الأطراف ذات العلاقة، تتضمن على سبيل المثال لا الحصر الفئات التالية: الرياضة وخدمات الترفيه والتسلية وخدمات التعليم وخدمات المشتركين لدى مشغلي الهاتف الجوال.

مما هو جدير الإشارة أن المرخص لهم بتقديم الرسائل القصيرة الجماعية قد ذكروا أنهم يتلقون فقط حوالي ١٠٠ شكوى في الشهر الواحد، بل إن بعضهم (١٧%) أفادوا أنه لا ترد إليهم أية شكاوى، وقد يعزى هذا إلى أن المستخدمين لا يعلمون من هو المنشئ الحقيقي للرسائل القصيرة التي وردت إليهم.

يتضمن الجدول أدناه ملخصاً للنتائج الرئيسية المستقاة من مسح الرسائل الاقتحامية:

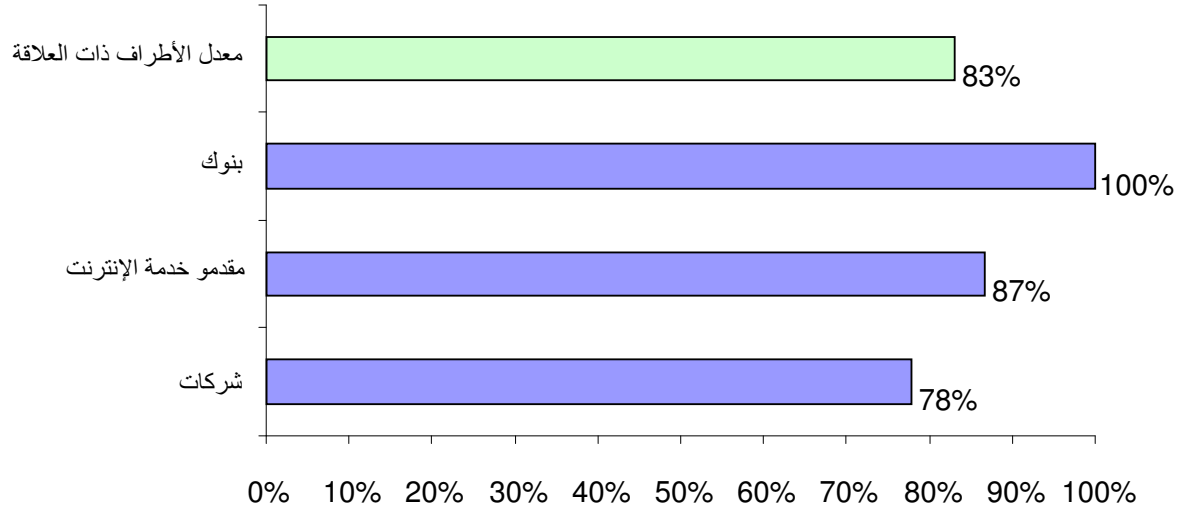
٦-٣ الطريقة المتبعة حالياً من الجهات ذات العلاقة لمكافحة الرسائل الاقتحامية

تحتاج معالجة قضية الرسائل الاقتحامية (SPAM)إلى منهج متعدد المستويات بدلاً من مجرد نشر أدوات ومصافي لمنع مرور الرسائل الاقتحامية، كما أن هناك حاجة إلى وضع عمليات مناسبة للتبليغ عن الرسائل الاقتحامية (SPAM)ومعالجتها مستوى عالي علاوة على توفر التوعية السليمة والتعليم للمستخدمين النهائيين والعملاء. ومن أجل تقديم رؤية شاملة حول كيفية المعالجة الحالية من قبل الأطراف ذات العلاقة للرسائل الاقتحامية في المملكة، فقد قمنا بدراسة ثلاثة مجالات.

أولاً، قمنا بدراسة الحلول المستخدمة حالياً لمكافحة الرسائل الاقتحامية، بما في ذلك المواقع الذي تم فيه نشر هذه الحلول وإعداداتها. ثانياً، قمنا بدراسة العمليات القائمة للسيطرة على الرسائل الاقتحامية (SPAM)وضبطها، بما في ذلك إجراءات تبليغ الجهات المختصة عن الرسائل الاقتحامية. ثالثا وأخيراً، قمنا ببحث ما إذا كانت الأطراف ذات العلاقة تنفذ برامج توعية بالرسائل الاقتحامية (SPAM)داخل مؤسساتها.

أدوات مكافحة الرسائل الاقتحامية

انطلاقاً من المسح الذي قمنا بإجرائه، اتضح جلياً أن الرسائل الاقتحامية (SPAM)تشكل قلقاً واهتماماً كبيراً لدى الجماعات ذات العلاقة التي تبنّت أنواعاً مختلفة من الحلول تتفاوت من الأدوات الأمنية العامة التي تقدم أيضاً حماية من الرسائل الاقتحامية (SPAM)وصولاً إلى أدوات ومصافي مكافحة الرسائل الاقتحامية (SPAM)المتطورة. تظهر إحصائياتنا أن متوسط النسبة المئوية للأطراف ذات العلاقة التي يتوفر لديها ضوابط تستهدف الرسائل الاقتحامية (SPAM)تعتبر مرتفعة جداً (٨٣%)، وقد قامت هذه الأطراف بنشر أدوات/مرشحات (Filters) مكافحة الرسائل الاقتحامية (SPAM)على شبكاتها لتصفية حركة الرسائل الواردة. يوضح الجدول أدناه النسبة المئوية لمختلف أنواع الأطراف ذات العلاقة.

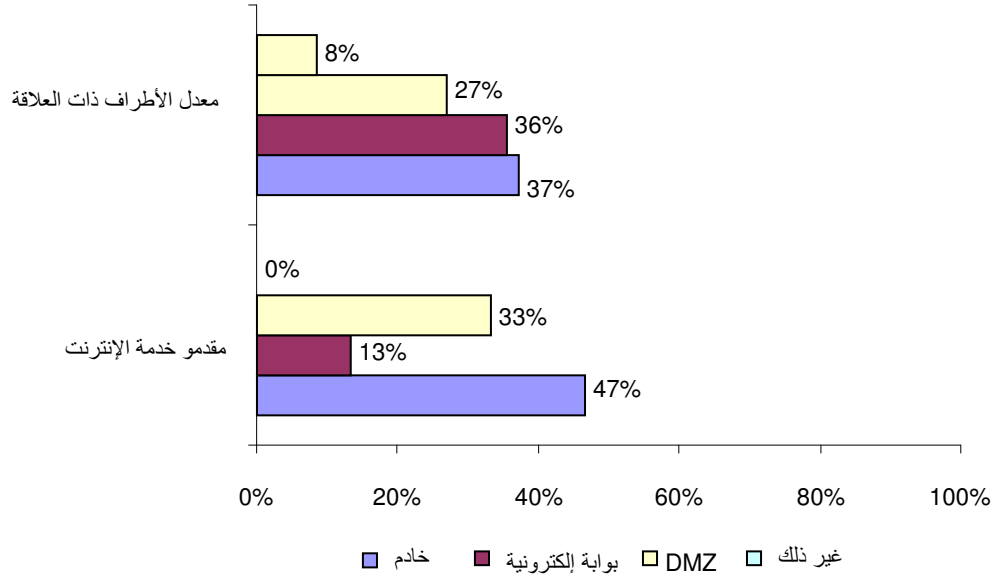


الشكل (٩): نسبة الأطراف التي ردت والتي تستخدم أدوات/مصافي للبريد الإلكتروني لمكافحة الرسائل الاقتحامية (SPAM)(الواردة)

ثمة نتيجة أخرى هامة كشفت عنها دراستنا تتعلق بالموقع الذي يتم فيه نشر حل مكافحة الرسائل الاقتحامية (SPAM)لتصفية حركة الرسائل الواردة. حيث اتضح أن نسبة متوازنة من الأطراف ذات العلاقة المستجيبين

للدراسة تقوم بنشر أدوات مكافحة الرسائل الاقتحامية (SPAM)على خوادمها[12] (٣٧%) وعلى بواباتها الإلكترونية (٣٦%).

لكن مثلما تمت الإشارة إليه أدناه، أن مزودي خدمة الانترنت يتجهون إلى أن تكون لديهم افكار مختلفة، حيث أن معظم مزودي خدمات الإنترنت يميلون إلى نشر حلول مكافحة الرسائل الاقتحامية (SPAM)على خوادمهم (٤٧%) ليتسنى لهم حماية صناديق البريد التي يحتفظون بها في خوادمهم، بينما يكون تركيز هؤلاء أقل على حماية أو تصفية الحركة المتجهة عبر شبكاتهم. هناك نسبة ١٣% فقط من مزودي خدمة الإنترنت يتجهون إلى نشر حلول مكافحة الرسائل الاقتحامية (SPAM)على بواباتهم الإلكترونية، وهذا يعني أن الرسائل الاقتحامية (SPAM)التي منشأها أو هدفها عملاء مزودي خدمات الإنترنت تستطيع المرور عبر شبكة مزودي خدمات الإنترنت دون كشفها أو تصفيتها.

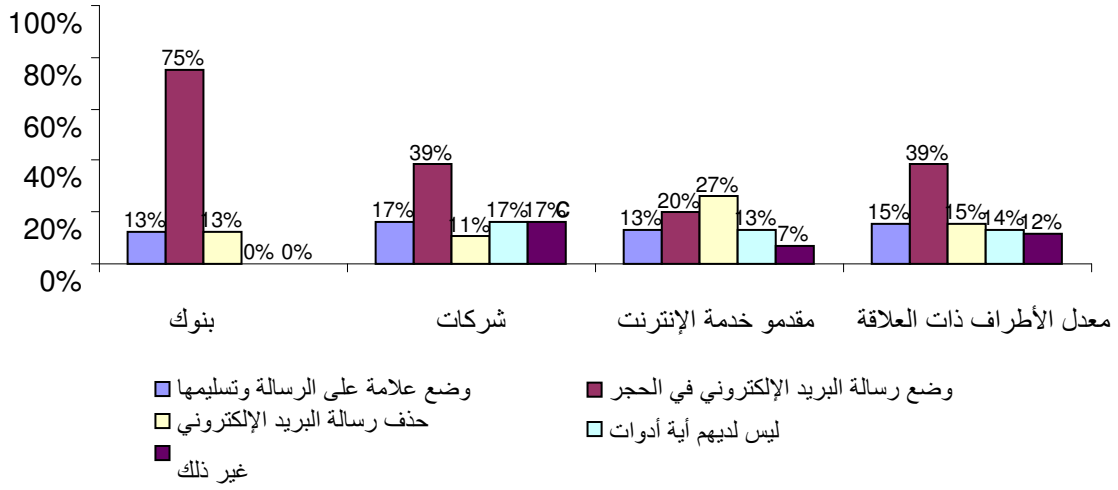


الشكل (١٠): نسبة الأطراف التي ردت والتي قامت بتركيب أدوات/مصافي خاصة بها للبريد الإلكتروني (الوارد) لمكافحة الرسائل الاقتحامية (SPAM)بحسب المعايير الموضحة في الشكل

يوضح الشكل-١١ أدناه أن البنوك والشركات تفضل حجر (Quarantined) رسائل البريد الإلكتروني الاقتحامية المشتبه فيها. من ناحية أخرى، نجد أن مزودي خدمات الإنترنت منقسمين حول ما إذا كان يتعين حذف رسائل البريد الإلكتروني المشتبه في أنها رسائل اقتحامية أم يتعين وضعها في الحجر.

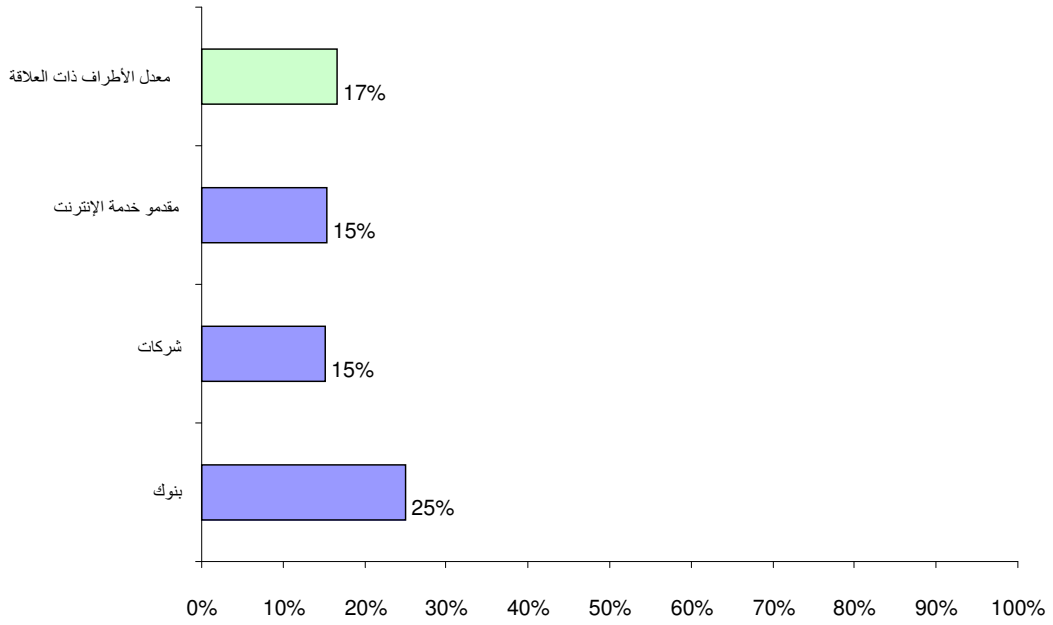
---

12 عند نشر أي حل لمكافحة الرسائل القصيرة على الخادم، يتم فقط فحص وتنظيف رسائل البريد الإلكتروني الواردة والصادرة. بينما عندما نشر الحل على البوابة الإلكترونية للشركة، فإنه يتم التفتيش على جميع حركة مرور البيانات الداخلة إلى الشبكة والخارجة منها وتنظيفها. وعلى سبيل المثال فإن الأجهزة الحاضنة (zobies) قد ترسل رسائل بريد إلكتروني تمر دون أن يتم التعرف إليها من خلال الحل الذي يركب على الخوادم.



الشكل (١١): نسبة الأطراف التي قامت بإعداد وتهيئة أدوات مكافحة الرسائل الاقتحامية (SPAM)لديها بحسب المعايير الموضحة في الشكل

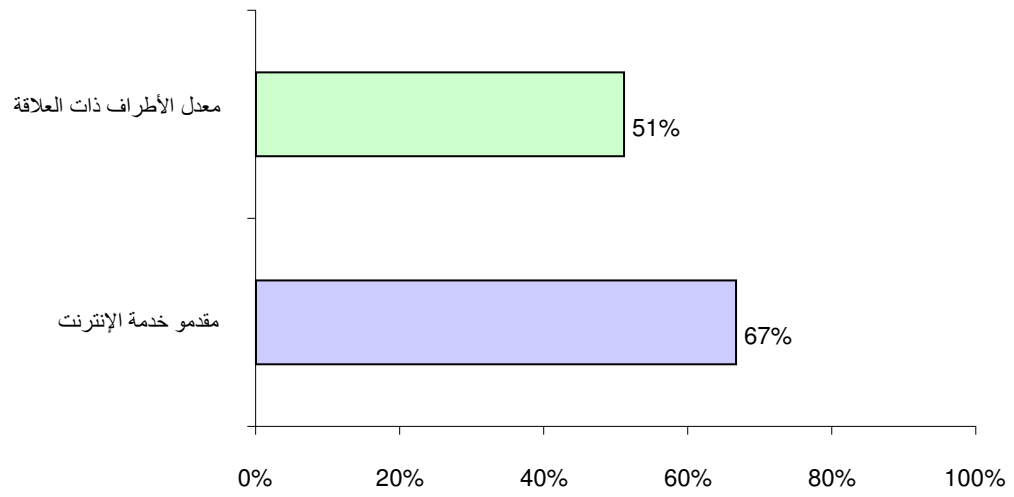
تُعتبر القوائم السوداء[١٣] (RBLs) فعالة في حجب نسبة كبيرة من رسائل البريد الإلكتروني الاقتحامية علماً أن هذه القوائم تحتاج إلى التحديث والصيانة بانتظام كي لا تقوم بحجب حركة البريد الشرعي من قبيل الصدفة. ومن جانبنا، قمنا خلال البحث بالتحقق مما إذا كانت الأطراف ذات العلاقة تستخدم قوائم سوداء في الحلول المقترحة من قبلهم لمكافحة الرسائل الاقتحامية. في الشكل-١٢ أدناه، نلاحظ في المتوسط أن نسبة ١٧% فقط من الأطراف ذات العلاقة تتجه إلى استخدام القوائم السوداء بصفة منفصلة عن حلولهم لمكافحة الرسائل الاقتحامية، أما فيما يتعلق بالبنوك، فالنسبة أعلى حيث تبلغ ٢٥%.



[13] القائمة السوداء المحدثة (RBL) هي قائمة لعناوين بروتوكول الإنترنت الذي يرفض أصحابها إيقاف نشاط الرسائل الاقتحامية عليها، وتقوم هذه القوائم السوداء بإدراج عناوين بروتوكول الإنترنت لمقدمي خدمة الإنترنت الذين يكون عملاؤهم مسئولين عن إرسال الرسائل الاقتحامية من مقدم الخدمة ذاك والذي تكون خوادمه قد أصبحت موئلاً وقاعدة لنقل الرسائل الاقتحامية.

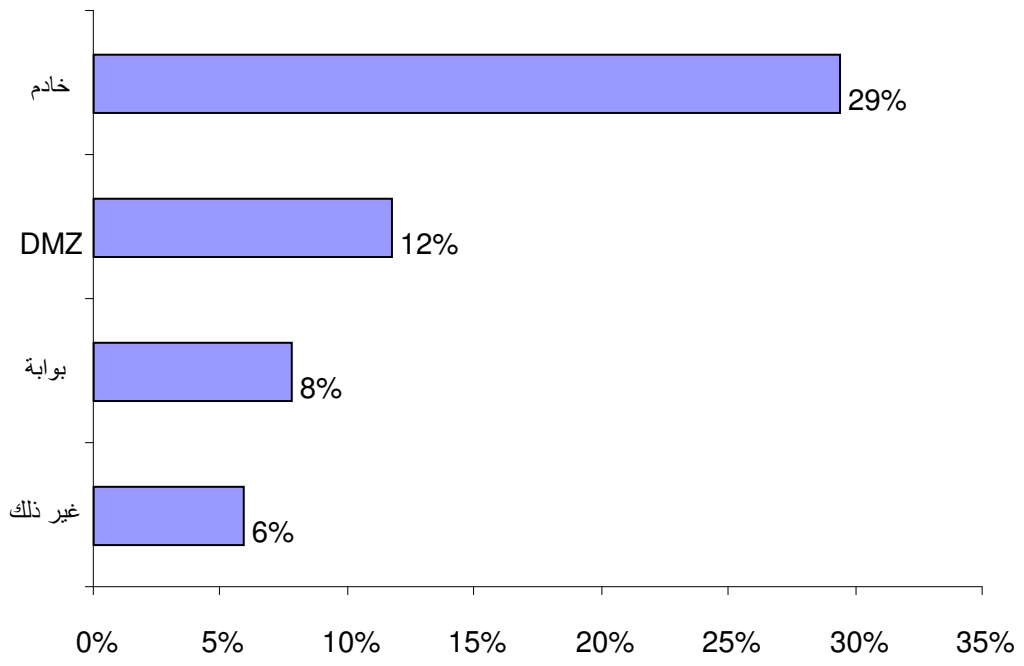
الشكل (١٢): نسبة الأطراف الذين قاموا بالرد ويستخدمون حلول القوائم السوداء (RBL) بشكل منفصل عن حلول مكافحة الرسائل الاقتحامية (SPAM)

بالنظر إلى حركة الرسائل الصادرة، فقد أظهر المسح أن الأطراف ذات العلاقة أقل اهتماماً باعتراض الرسائل الاقتحامية (SPAM)على حركة بريدهم الصادر، وفي المتوسط يعمل ٥١% من الأطراف ذات العلاقة على نشر حلول لتصفية حركة بريدهم الصادر بالمقارنة مع ٨٣% من الأطراف ذات العلاقة التي تقوم بتصفية حركة بريدهم الوارد. هذا الواقع يوضح أن الأطراف ذات العلاقة ليست مفرطة في قلقها من الرسائل الاقتحامية (SPAM)التي قد تصدر من شبكاتها. وبالنسبة لمقدمي خدمات الإنترنت، فبالإضافة إلى كون معظمهم لا يعملون على تصفية حركة البريد الإلكتروني المرسل من قبل عملائهم دون المرور عبر خادم البريد الإلكتروني التابع لمقدم الخدمة، فإن معظم مقدمي خدمات الإنترنت لا يقومون بفحص خوادم (Mail Gateways) البريد الإلكتروني التابعة لهم للتحقق مما إذا كانت تلك الخوادم تقوم بإصدار رسائل اقتحامية، ويوضح الشكل-١٣ أدناه هذه النقطة.

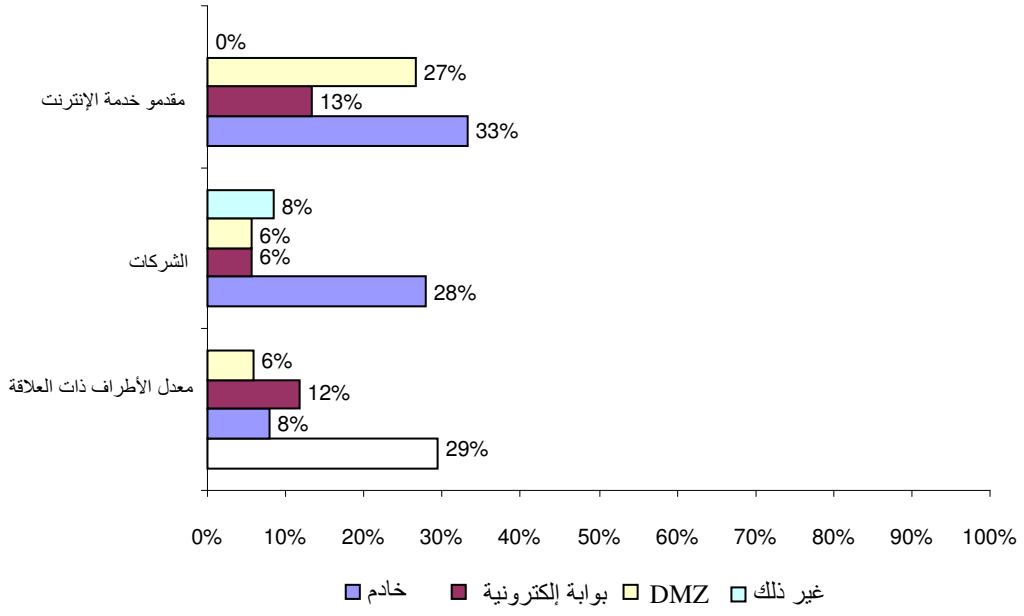


الشكل (١٣): نسبة الأطراف التي ردت والتي تستخدم أدوات/مصافي لمكافحة رسائل البريد الالكتروني الاقتحامية (الصادرة)

فيما يتعلق بالموقع الذي يتم فيه تركيب الأدوات على حركة البريد الإلكتروني الصادر، فإن دراستنا توضح أن نسبة ٨% فقط من متوسط الأطراف ذات العلاقة مهتمة بحماية الحركة الصادرة على بواباتها الإلكترونية، وفيما يختص بمقدمي خدمات الإنترنت فإن نسبة ١٣% فقط مهتمة بحماية الحركة الخارجة من بواباتها الإلكترونية. هذا يعني أنه في حال قيام أحد المشتركين بتركيب خادم بريد، فإن بإمكانه إرسال رسائل بريد إلكتروني اقتحامية دون كشفه. بالإضافة إلى ذلك، هذا يعني أن بإمكان مرسلي الرسائل الاقتحامية (SPAM)إرسال رسائل اقتحامية دون أن يتم اكتشافهم. ويقدم الشكلان (١٤) و (١٥) صورة أوضح عن هذا الوضع.



الشكل (١٤): نسبة الأطراف التي ردت والتي قامت بتركيب أدوات/مصافي خاصة بها لمكافحة رسائل البريد الالكتروني الاقتحامية (الصادرة) بحسب المعايير الموضحة في الشكل



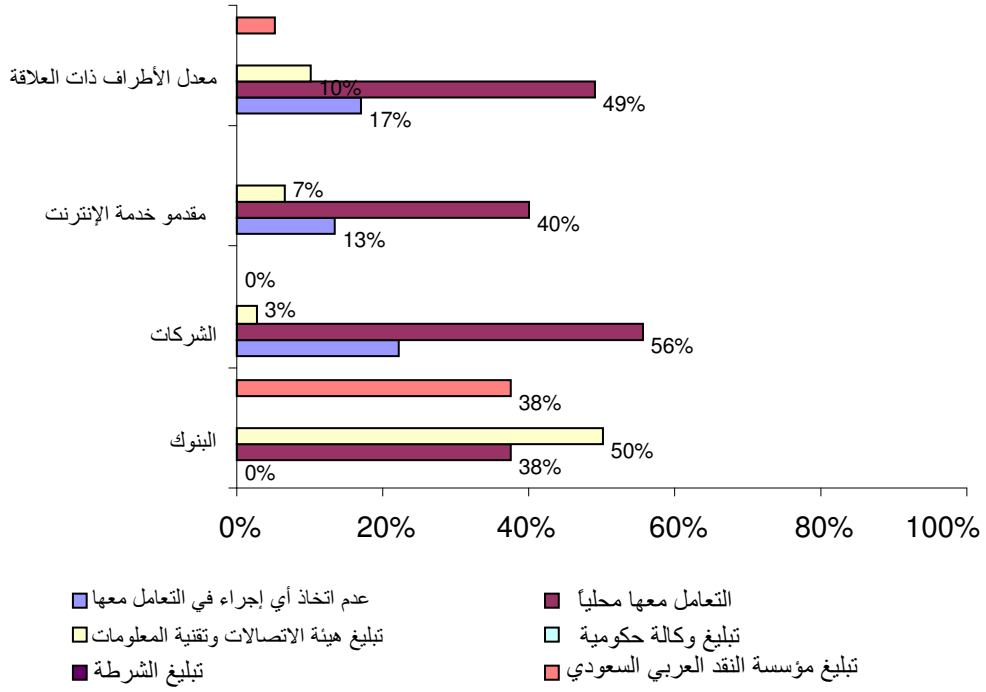
الشكل (١٥): نسبة الأطراف التي ردت والتي قامت بتركيب أدوات/مصافي خاصة بها لمكافحة رسائل البريد الالكتروني الاقتحامية (الصادرة) بحسب المعايير الموضحة في الشكل وبحسب نوع الطرف ذي العلاقة

عمليات ضبط الرسائل الاقتحامية

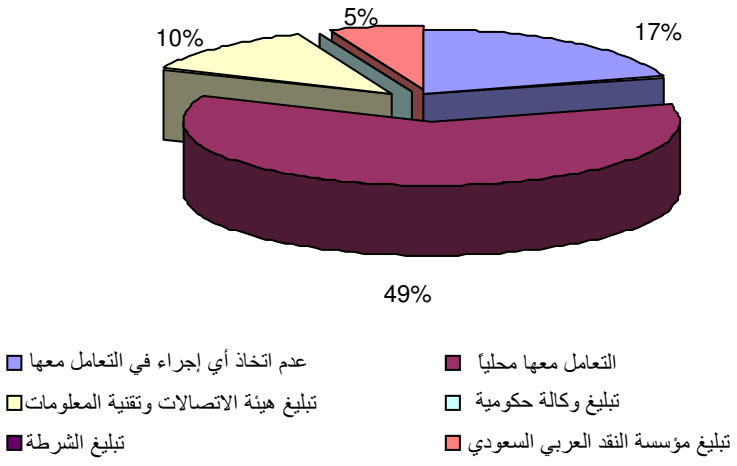
تمثل الجانب الثاني الذي شملته دراستنا في العمليات المستخدمة لدى الأطراف ذات العلاقة للسيطرة على وضبط الرسائل الاقتحامية، ويتضمن ذلك التعامل مبدئياً مع الرسالة الاقتحامية، إجراءات التبليغ عن الرسائل الاقتحامية، سياسات الاستخدام المقبول مع العملاء، ولائحة الضوابط السلوكية التي تحكم التعامل بين الأطراف المختلفة.

أوضحت دراستنا أنه في ظل عدم وجود عملية تبليغ رسمية للشكاوى المتعلقة بالرسائل الاقتحامية، فإنه ليس من الغرابة (باستثناء البنوك) أن معظم المؤسسات تتعامل مع الرسائل الاقتحامية (SPAM)على المستوى الداخلي فقط، أو أنها لا تتخذ أي إجراء حيال الشكاوي المتعلقة بالرسائل الاقتحامية، بل إن نسبة ١٧% من الأطراف ذات العلاقة لا توجد لديها حتى عمليات ملائمة للتعامل مع الرسائل الاقتحامية (SPAM)حسبما يتضح في الشكلين (١٦) و (١٧) أدناه.

لكن الوضع يختلف لدى البنوك. فالشكل-١٦ يوضح أن حوالي نصف البنوك لديها إجراءات للتبليغ عن شكاوى التزوير والاحتيال إلى هيئة الاتصالات وتقنية المعلومات (CITC) ومؤسسة النقد العربي السعودي(SAMA). كما أنه من خلال وضع هيكلية لمكافحة الرسائل الاقتحامية، فمن المتوقع أن تطور القطاعات الأخرى مثل هذه العمليات لديها وإجراءات التبليغ عن الرسائل الاقتحامية.



الشكل (١٦): نسبة الأطراف ذات العلاقة التي اتخذت أحد الإجراءات الموضحة في الشكل عند اكتشاف رسائل اقتحامية - بحسب نوع الطرف ذي العلاقة



الشكل (١٧): نسبة الأطراف ذات العلاقة التي اتخذت أحد الإجراءات الموضحة في الشكل عند اكتشاف رسائل اقتحامية

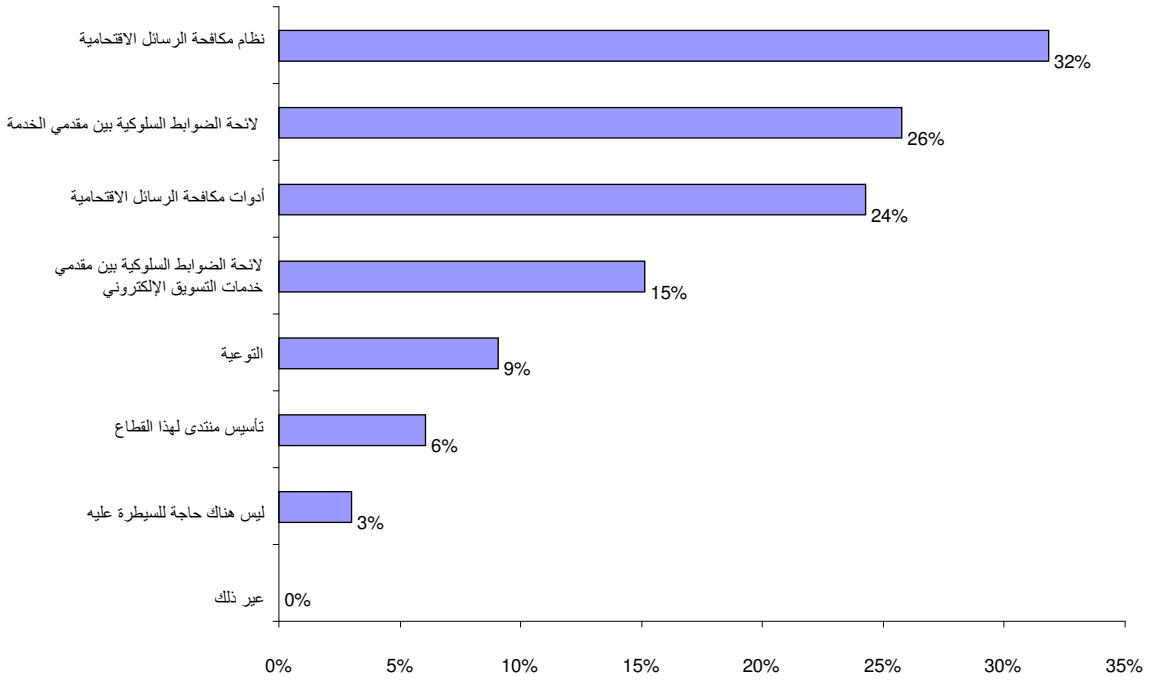
لقد حاولنا ضمن مسح دراستنا تأكيد أراء الأطراف ذات العلاقة حول أفضل الطرق لمكافحة الرسائل الاقتحامية، وقد أشرنا إلى ذلك في الشكل-١٨ أدناه:

- ٣٢% من الأطراف ذات العلاقة ترى أن وجود نظام لمكافحة الرسائل الاقتحامية (SPAM)هو الأسلوب الأكثر فاعلية الذي سيتسنى من خلاله للمؤسسات مكافحة الرسائل الاقتحامية.
- ٢٦% من الأطراف ذات العلاقة توافق أيضاً أن وجود لائحة للضوابط السلوكية بين مقدمي الخدمات سوف يساعد كثيراً على منع الرسائل الاقتحامية (SPAM)على الرغم من أن ١٣% فقط من مقدمي خدمات الإنترنت يعتقدون أن وجود لائحة للضوابط السلوكية سوف يساعد على مكافحة الرسائل الاقتحامية[١٤].
- ٢٤% من الأطراف ذات العلاقة (خاصة مقدمي خدمات الإنترنت والشركات) ترى أن نشر أدوات مكافحة الرسائل الاقتحامية (SPAM)كان إجراءً كافياً لمنع الرسائل الاقتحامية.
- ١٥% وافقوا على أن وجود لوائح صارمة للتسويق الإلكتروني بما فيها احتمال وجود لائحة للضوابط السلوكية بين مزودي خدمات التسويق الإلكتروني يمكن أن يساعد على السيطرة على وضبط الرسائل الاقتحامية[١٥].

---

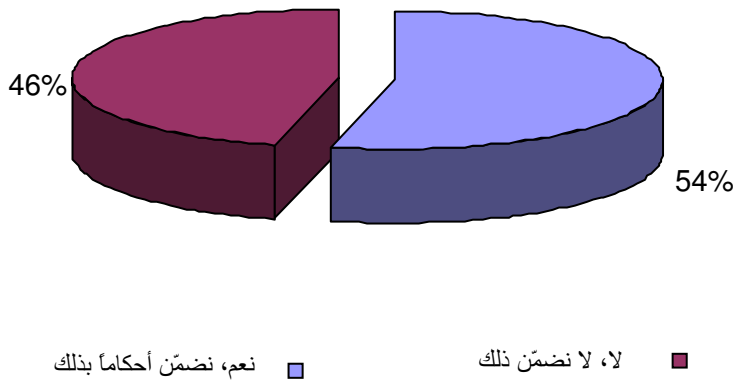
[14] قد يكون ذلك ناجحاً لأن مقدمي خدمة الإنترنت يدركون أن وجود لائحة للضوابط السلوكية بدون آلية لتنفيذها ومراجعتها لن تساعد في الحد من نسبة الرسائل الاقتحامية

[15] هذا يعكس أهمية مساعدة القطاع في المعركة ضد الرسائل الاقتحامية. وعلى الرغم من أهمية التشريعات، فإن وجود إرشادات محددة للقطاع تكون مصممة وفقاً الاحتياجات ذلك القطاع يعتبر أمراً في غاية الأهمية.

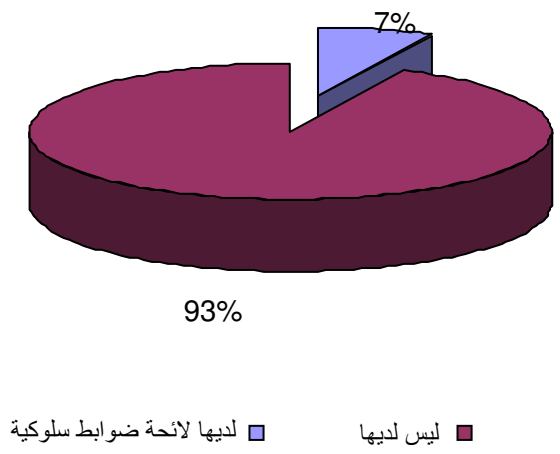


الشكل (١٨): وجهة نظر الأطراف ذات العلاقة حول كيفية مكافحة الرسائل الاقتحامية (SPAM)

هذا الأمر يقودنا إلى النظر في اثنين من الجوانب الأخرى: هل يضمن مقدمو الخدمات أن عملاءهم لا يسيئون استخدام الخدمات المقدمة لهم؟؛ وهل يتعاون مقدمو الخدمات مع بعضهم البعض في مكافحة الرسائل الاقتحامية؟. أولاً، لاحظنا من واقع المسح أن ٤٦% منهم لا تتوفر لديهم أي أحكام لمكافحة الرسائل الاقتحامية (SPAM)في سياسة الاستخدام المقبول، علماً أن إضافة هذه الأحكام يمكن أن يساعد كثيراً في ضبط الرسائل الاقتحامية (SPAM)التي منشأها المملكة العربية السعودية. ثانياً، اكتشفنا أيضاً أن نسبة ٩٣% من مزودي الخدمات (الشكل-٢٠) ليس لديهم إلمام فيما إذا كان هناك أية لائحة ضوابط سلوكية بين مزودي الخدمات، وهذا يعني عدم وجود تعاون بين مقدمي الخدمات لضبط والسيطرة على الرسائل الاقتحامية.



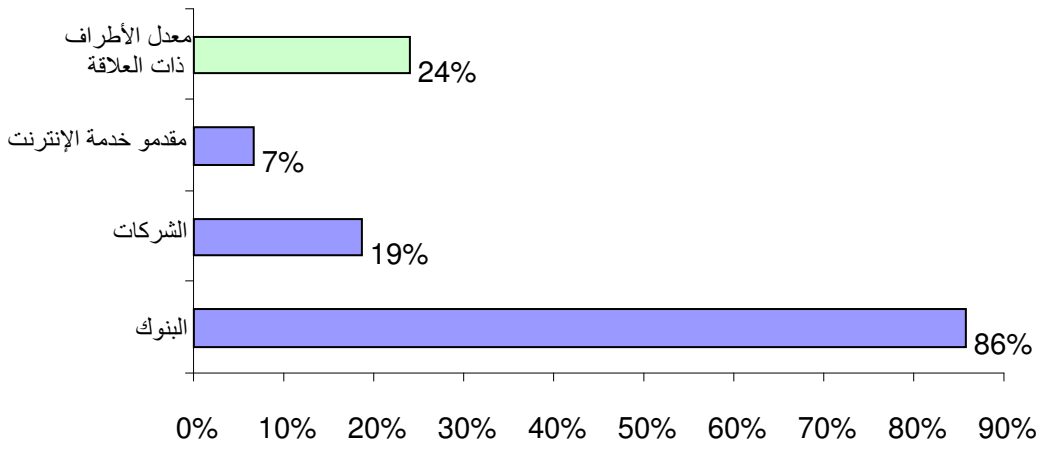
الشكل (١٩): هل تضمّنون أحكاما في القسم الخاص بالاستخدام المقبول في العقود بشأن القيود على إرسال الرسائل الاقتحامية؟



الشكل (٢٠): وجود لوائح داخلية لضبط السلوك المهني لدى مزودي خدمة الإنترنت فيما يتعلق بالرسائل الاقتحامية (SPAM)

برامج التوعية بالرسائل الاقتحامية

أخيراً، لقد حاولنا في بحثنا هذا تحديد مستوى التوعية التي تقدمها الجماعات ذات العلاقة إلى عملائها ومنسوبيها، وكانت النتائج مثيرة للدهشة مثلما نلاحظ في الجدول (٢١) أدناه. فمتوسط الجماعات ذات العلاقة البالغ ٢٤% يشير إلى أن المؤسسات لا تبذل الكثير من الجهد في تثقيف عملائها والعاملين لديها حول كيفية التعامل مع الرسائل الاقتحامية. غير أن البنوك سجلت نسبة عالية في هذا الجانب بلغت ٨٦% في إقامة برامج توعية لموظفيها وعملائها.



الشكل (٢٠): الأطراف ذات العلاقة التي تستخدم برامج توعية بالرسائل الاقتحامية