**المقدمة:**

**ما المقصود بأمن المعلومات ؟ وما أهميته لدى البنوك ؟**

يقصد بأمن المعلومات: مجموعة من العمليات والإجراءات والأدوات التي تتخذها القطاعات أو المنظمات لتأمين وحماية معلوماتها وأنظمتها ووسائطها من وصول غير المصرح لهم , سواء في لمن هم داخل القطاع أو خارجه.

يشكل أمن المعلومات على مستوى العالم هاجساً وقلقاً بالنسبة للقائمين على إدارة الأنظمة المعلوماتية المختلفة، لاسيما في ظل تنامي عمليات الجرائم المعلوماتية التي فرضت الحاجة إلى تضافر جهود جميع الدول والمؤسسات الحكومية والخاصة على مستوى العالم، بما في ذلك الأفراد، للقضاء على كل ما يخل بأمن المعلومات، وبالذات في ظل تطور التقنية وانتشار المخاطر التي تكتنف استخداماتها وتطبيقاتها المختلفة.

ويعرف مصطلح أمن المعلومات بمفهومه الواسع والشامل على أنه مجموعة من الإجراءات التي تمكن صاحب المعلومة من إبقاء معلوماته الشخصية وبياناته وحساباته المالية والمصرفية تحت سيطرته الكاملة والمباشرة، وعدم السماح لأي شخص غير مرخص له بالوصول إليها بهدف تداولها سواء بحسن نية أو بسوء نية أو بهدف الابتزاز والعبث بها. وعادة ما تحدث الاختلالات الأمنية في أنظمة أمن المعلومات عندما تتعرض الأنظمة لاختراقات من خلال مثلاً ما يعرف بالمتسللين الـ (هاكرز) أو بالفيروسات أو أي نوع آخر من أنواع البرامج الخبيثة.

ويسعى المختصون في أمن المعلومات إلى ضمان سلامة أنظمة المعلومات المختلفة من خلال تحقيق ثلاثة مطالب أساسية، تتمثل في سرية المعلومات، سلامة المعلومة، وتوافر المعلومة.

1. ويتطلب تحقيق المطلب الأول المرتبط بسرية المعلومات تأمين المعلومات بشكل يمكن فقط الأشخاص المصرح لهم الوصول إليها دون غيرهم (أصحاب الصلاحية أو المخول لهم).
2. أما المطلب الثاني المتمثل في سرية المعلومة، فيسعى إلى ضمان سلامة مصادر المعلومات، بحيث لا يمكن تغييرها أو تحديثها إلا من قبل الأشخاص المصرح لهم فقط.
3. فيما المطلب الثالث لضمان أمن المعلومات فيتمثل في إمكانية وسهولة توفير المعلومات وقت الحاجة إليها. كما أن هناك عددا من العناصر التي تتسبب في إضعاف نظم أمن شبكات الاتصال المختلفة وفي سرقة المعلومات، والتي من بينها على سبيل المثال، تسريب كلمات السر، التصنت الإلكتروني، الاختراق، الفيروسات، الاستدراج، وسرقة الهوية.

ومن هذا المنطلق نعرف الأهمية القصوى التي استوجبت اهتمام الدول والمؤسسات الحكومية والخاصة والأفراد , وفي ظل تطور التقنية وانتشار المخاطر التي باتت تؤرق المجتمعات فالتقنية رغم ما تقدمه من خدمات جليلة للإنسان في العصر الحديث إلا أنها وكأي اختراع آخر لها محاسنها الكثر ولها سلبياتها الخطيرة اذا لم التعرف عليها والعمل على تفاديها , وفي إطار بحثنا هذا سنتطرق إلى طرق وأدوات لحماية أمن المعلومات للمستخدم العادي في البنوك المصرفية.

**أمن الخدمات المصرفية للبنوك على الإنترنت :**

برغم التطور المذهل الذي طال الخدمات المصرفية الإلكترونية بشكل عام والخدمات المصرفية عبر الإنترنت بشكل خاص، إلا أنه لا تزال هناك جملة من التحديات أمام المصارف في مجال التقنية البنكية، التي تتمثل في قدرتها على المحافظة على أمن وسلامة المعلومات، بما في ذلك التعامل مع المخاطر التشغيلية وسد الثغرات، وبالذات في ظل انتشار وتزايد أعداد جرائم المعلوماتية والجرائم الإلكترونية على مستوى العالم.

أمام ذلك، أصدرت مؤسسة النقد العربي السعودي ''ساما'' تعليمات مشددة تقتضي من جميع البنوك العاملة في المملكة الالتزام بها للتأكد من حماية أنظمة وأصول المعلومات من أي تعديل أو إتلاف أو نسخ من قبل أي شخص ليست لديه الصلاحية بذلك، سواء كان ذلك الشخص متعمداً أو غير متعمد.

وفي مجال تعزيز قدرات تقنية المعلومات البنكية والمحافظة على جودتها ونوعيتها وسريتها، أجرت مؤسسة النقد فحصا لجميع البنوك المحلية للتأكد من توفر الأنظمة الرقابية والأمان للعمليات البنكية من خلال الهاتف البنكي والإنترنت، إضافة إلى دراسة الشكاوى التقنية المتعلقة بالخدمات البنكية عن طريق الإنترنت، وتطوير ضوابط تعزيز أمن العمليات البنكية من خلال الهاتف البنكي، وتزويد البنوك بالمقترحات التي تساعد على عملية الوقاية من التعرض والاستغلال في تنفيذ جرائم غسل الأموال وتمويل الإرهاب.

كما درست ''ساما'' بعض جوانب الإجراءات الأمنية لأنظمة الخدمات البنكية الإلكترونية التي تقدمها البنوك لعملائها، وتوجيه البنوك بإضافة أو تعديل بعض منها لتتواكب مع أحدث وسائل الحماية الأمنية في هذا الشأن، بهدف تحقيق المزيد من الأمن والحماية لحسابات العملاء.

ومن أنظمة مؤسسة النقد العربي السعودي:

1. نظام المعلومات الائتمانية.
2. نظام مكافحة غسل الأموال.
3. نظام مكافحة التزوير.
4. نظام النقد.
5. نظام مؤسسة النقد العربي السعودي.
6. نظام مراقبة البنوك. ]1[

وعلى هذا فقد سعت البنوك إلى تطبيق هذه المعايير لحماية عملاءها وتوعيتهم حول ما قد يصيبهم من المخترقين.

* **البنك العربي**

**سياسة أمن المعلومات**

**أمن معلوماتك**

إن المحافظة على سرية وأمن معلوماتك الشخصية من أهم الأولويات في البنك العربي حيث اتخذنا التدابير المناسبة لحماية سرية معلوماتك الشخصية ووقايتها من الدخول غير المصرح به، إذ أن حماية معلوماتك الشخصية تعتبر مسئولية كل موظف من موظفينا.

ويقوم البنك العربي بشكل متواصل بمتابعة التطورات المتعلقة بحماية المعلومات وتحديث عملياته وإجراءاته لضمان الالتزام بأعلى ممارسات الصناعة المصرفية في هذا المجال. وسواء اخترت التعامل معنا من خلال مراكزنا المالية/فروعنا، أو أجهزة الصراف الآلي، أو الخدمات المصرفية عبر البنك الناطق أو الإنترنت، فإننا نلتزم بالمحافظة على حماية معلوماتك سواء عند جمعها أو استخدامها أو مشاركتها.

للحصول على معلومات إضافية حول إجراءاتنا لحمايتنا خصوصية المعلومات، يرجى الضغط على الرابط التالي [سياسة خصوصية المعلومات](http://www.arabbank.com/ar/privacypolicy.aspx) في البنك العربي.

**حماية كلمة السر**

تعتبر كلمات السر المفاتيح إلى حساباتك ومعلوماتك الشخصية. وفيما يلي بعض الخطوات التي يمكنك القيام بها لحماية معلوماتك الشخصية من الدخول غير المصرح به.

|  |  |
| --- | --- |
| **اعمل** | **لا تعمل** |
| \* استخدم ستة حروف على الأقل  \* استخدم حروف وأرقام  \* استخدم أحرفا خاصة إذا كان بالإمكان(@#&$) \* استخدم الحروف الكبيرة والصغيرة (A a) \* قم بتوحيد الكلمات في كلمة واحدة أو استخدم تهجئه خاطئة \* قم بالتغطية أثناء إدخال كلمة السر  \* غير كلمة السر بشكل دوري | \* لا تستخدم أسماء أشخاص  \* لا تستخدم معلومات شخصية  \* لا تستخدم كلمات من القاموس  \* لا تكتبها على ورق لاصق ولا تحفظها على شاشة الحاسوب \* لا تحفظ كلمة السر في الدرج  \* لا تستخدم نفس كلمة السر لعدة تطبيقات  \* لا تعيد استخدام كلمات السر القديمة |

**أحذر من سرقة بياناتك الشخصية عبر الإنترنت "Phishing"**

هو نوع من أنواع الخداع المعد للحصول واستخدام معلوماتك الشخصية واستخدامها (مثل أرقام بطاقات الائتمان، كلمات السر، بيانات حسابك، الخ) لأغراض احتيالية.

قد يقوم محترفو الاحتيال عبر الانترنت (قراصنة الانترنت) بإرسال الآلاف من الرسائل الإلكترونية المزيفة التي يبدو وكأنها صادرة عن مواقع الكترونية موثوقة، مثل الموقع الخاص بالبنك الذي تتعامل معه أو موقع شركة بطاقة ائتمانك، حيث تطلب هذه الرسائل الإلكترونية إعطاء معلومات شخصية عنك من خلال البريد الإلكتروني أو على موقع غير مشروع على شبكة الإنترنت يكون منشئا من قبل هؤلاء القراصنة لغايات احتيالية.

**نصائح لحمايتك من سرقة بياناتك الشخصية عبر الإنترنت "Phishing"**

في حالة استلامك رسالة الإلكترونية مشكوك فيها بحيث تبدو أنها صادرة عن البنك العربي، يرجى القيام بما يلي:

* لا تقم بالرد على الرسالة، أو بالنقر على أي رابط إلكتروني، أو بأجراء اية تغييرات على الرسالـة الإلكترونية بأية طريقة.
* [اتصال بنا](mailto:ArabBankGroup.RegulatoryCompliance@Arabbank.com.jo) فورا وقم بشطب رسالة البريد الإلكتروني بعد تبليغنا عنها .
* قم بالتأكد من أن برنامج الحماية من الفيروسات وبرامج الحماية من التجسس الإلكتروني " anti-spyware" محدثة وخاصة إذا قمت بالنقر بالخطأ على الرابط أو المرفـق بالرسالـة الإلكترونية.

**نصائح أخرى لحماية معلوماتك الشخصية**

* كن شديد الحذر عند التسوق عبر الإنترنت. لا تقم بإدخال رقم بطاقة الائتمان أو معلوماتك الشخصية إلا إذا قمت أنت بإنشاء هذه العملية وعلى موقع الكتروني موثوق.
* عند إدخالك لأرقام بطاقة الائتمان أو معلوماتك الشخصية تأكد من انك تستخدم موقعا الكترونيا آمنا. تأكد من وجود شهادة حماية أمنية للموقع الالكتروني قبل إدخال معلوماتك الشخصيـة.
* استخدم الخدمات المصرفية الإلكترونية بشكل منتظم (ومثالها: الخدمات المصرفية عبر الإنترنت أو الهاتف النقال "SMS" أو البنك الناطق أو عن طريق أجهزة الصراف الآلي "ATM") للكشف عن أية عمليات احتيالية إن وجدت.
* أغلق الرابط الإلكتروني على الشبكة عند الانتهاء من استخدامه وخاصة إذا كنت تستخدم المودم أو DSL للدخول إلى شبكة الإنترنت. ادرس إمكانية استخدام برنامج الحماية الشخصي (Personal Firewall).

**كيف نقوم بحمايتك؟**

**حماية أمن المعلومات**

ان الحفاظ على سرية وأمن معلوماتك الشخصية والمالية من أهم المسؤوليات المناط بنا. ستبقى معلوماتك في حماية نظرا للتدابير الأمنية المتخذة مثل: التشفير/الترميز، وتوثيق الدخول، وبرامج الحماية من الفيروسات، وبرامج كشف الدخول غير المصرح به، الموجودة الأنظمة والخدمات التي نقدمها . ]2[

**أنظمة لحماية البطاقات البنكية:**

**حماية ثلاثية الأبعاد (بنك الرياض):**

تجربة أكثر أماناً للتسوق عبر الانترنت فقط لأجلك!

من الآن فصاعداً، لن تحتاج للتسجيل عند تسوقك عبر الانترنت من المواقع التي تدعم خاصية الحماية ثلاثية الأبعاد ولا حاجة لحفظ اسم المستخدم والرقم السري الخاصين بك.

في كل مرة تقوم بعملية شراء عبر الانترنت في المواقع التي تحمل علامة "Verified by VISA" أو "MasterCard Secure Code".

سوف نرسل إلى رقم الجوال الخاص بك المسجل لدى بنك الرياض رقماً سرياً تستعمله لمرة واحدة فقط لإتمام عملية الشراء. وبهذا سوف تحمي بطاقتك الائتمانية من عمليات الاحتيال الالكترونية وستجعل تجربة التسوق عبر الانترنت أكثر أماناً.

### نصائح لتسوق آمن عبر الانترنت

التسوق عبر الانترنت سريع و سهل ومريح ولكن لاتزال هناك بعض عوامل السلامة التي يجب أخذها في الاعتبار عند استخدامك لبطاقة بنك الرياض الائتمانية في التسوق الإلكتروني عبر الانترنت.

* استخدم بطاقتك الائتمانية من بنك الرياض فقط في المواقع الموثوقة والمعرفة بأنها من المواقع الآمنة (ابحث عن صورة القفل في شريط الأدوات).
* في الصفحة التي تطلب إدخال معلومات بطاقتك الائتمانية ومعلومات شخصية أخرى تأكد أن عنوان الصفحة نفسها مشفر ويبدأ على النحو التالي https://. التشفير هو مقياس آمن يحفظ معلوماتك كما أدخلتها تماما.
* تأكد من أن الموقع حقيقي وآمن بمعرفة ماذا يقول عنه المتسوقون الآخرون. بعض المواقع الالكترونية مثل [epinions.com](http://epinions.com) و [bizrate.com](http://bizrate.com) تحتوي على تقييم المتسوقين، حيث تساعدك في تحديد شرعية الشركة.
* لا ترسل رسائل بريد الكتروني تحتوي على معلومات شخصية مثل رقم بطاقتك الائتمانية و تاريخ الانتهاء.
* استخدم برامج حماية جيدة ضد الفيروسات . ]3[

**ومن أجل حماية المستخدمين:**

* ترفض بعض البنوك العمليات في المواقع المشبوهة.
* عند تكرر العملية أكثر من مرة يقوم البنك بإيقاف البطاقة خوفا من أن تكون مسروقة.
* شركة فيزا العالمية لا تعترف إلا بالمواقع العالمية الموثوقة.

# 16 نصيحة لحماية حاملي البطاقات الائتمانية من الاحتيال والسرقة:

**1**- قم بحساب وتجهيز المبالغ النقدية قبل الوصول إلى جهاز الإيداع النقدي لتقليل الوقت الذي تقضيه عند الجهاز ويفضل الإيداع بإحدى فروع البنك ل تفادي حدوث المشاكل او تعرضك للسرقة

2- قم باتخاذ احتياطات الأمن والسلامة عند استخدام جهاز الصراف الآلي Drive thru وتجنب الصرف في أوقات متأخرة.

3 - غطِ شاشة الصراف الآلي ولوحة المفاتيح بطريقة لا يستطيع من ينتظر ورائك رؤية رقمك السري أو مبلغ العملية الذي أدخلته.

4- إذا اضطررت لإلغاء بطاقة الصراف الآلي الخاصة بك، اقطعها إلى أربعة أجزاء بشكل مائل عبر الشريط الممغنط ل ضمان عدم إساءة استخدام البطاقة.

5- عدم قبول أية تعليمات أو توجيهات، من أي طرف للذهاب إلى الصراف الآلي أو الدخول إلى خدمة المصرفية الإلكترونية عبر الإنترنت (المباشر)

6 – عليك بحفظ رقمك السري عن ظهر غيب و لا تكتبه في أي مكان حفاظاً عليه.

7 - تأكد أن عمليات السحب تتم بوجودك و تكون على علم بها

8 - لا ترسل رقم بطاقتك الائتمانية عبر البريد الالكتروني أو الهاتف الجوال إذا لم تتأكد بأنه امن

9 - عليك بإخبار البنك فور تغييرك رقم جوالك المسجل لديه، حتى يتمكن البنك من إرسال رسالة لك بالعمليات المدينة التي تتم على بطاقاتك الائتمانية على رقم هاتف جوالك الصحيح.

10 - أيضا عليك بإخبار البنك بأي تغيير يحدث على عنوانك البريدي الذي عادة ما يصلك من خلاله كشف حساب بطاقاتك الائتمانية، لان الكشف يحتوي على معلومات مهمة وحساسة، والتي تستوجب تحديث معلومات بريدك بحيث يتمكن البنك من إرسال الكشف على العنوان الصحيح.

11 - لا تستخدم أرقاماً سرية لبطاقتك المصرفية يمكن الكشف عنها بسهولة، مثل تاريخ الميلاد أو أرقام هاتفك الشخصي أو أرقام متسلسلة ومتكررة.

12 -  عليك التأكد من استخدام مواقع دفع آمنة ونظامية لدى استخدامك لبطاقتك عبر الشبكة العنكبوتية.

13 - يجب عليك الابتعاد عن أجهزة الكمبيوتر الموجودة في   مراكز الترفيه العامة أو المقاهي حين تنوي استخدامها لتنفيذ عمليات بنكية أو شرائية.

14 - تأكد من أن جهاز الحاسوب الخاص بك يحتوي على حماية ضد الفيروسات وضد الاختراق حتى يقوم بحماية بياناتك عند تنفيذ عملياتك البنكية.

15 - قم بتغيير أرقام بطاقتك السرية دورياً وبالذات لدى عودتك من السفر للخارج.

16 -  يجب أن يكون لديك إلمام تام بجميع عناصر الأمان الخاصة ببطاقات الدفع الإلكتروني بشكل عام، والبطاقات الائتمانية بشكل خاص.

### تعرف على السبام كي تحمي نفسك منه:

### 

لاشك ان العديد من الناس يتساءلون , كيف يقوم السبامر باختراق حسابات البايبال و البنوك , رغم قوة نظام الحماية في هذه المواقع.

يا ترى ما هو السبام ؟؟

السبام هو عملية يبدل فيها السبامر كل جهده للإسقاط بالضحايا و إقناعه بإدخال معلوماته البنكية أو حسابه في البايبال .

ويستعمل السبامر عدة ادوات لإنشاء صفحة السبام وجلب الضحايا الكثير . واغلب السبامر يشترون هذه الأدوات بمقابل مادي . وذلك ليحتالوا على الناس . سنشرح لكم بعض هذه الأدوات.

ما هي اأوات السبام ؟؟

1\_السكاما Scama

هذه الأداة هي كل شيء في السبام فهي الصفحة التي ينشئها السبامر لإسقاط بضحية وغالبا ما تكون صفحة بايبال . وهي تلعب الدور الرئيسي في نجاح أو فشل السبام

2\_سيبانيل Cepanel

وهو يلعب دور الاستضافة , يمكنك من رفع السكاما عليه و إنشاء صفحتك , وهو يعطيك دومين مجاني مرتبط ب بايبال ليسهل عليك جلب الضحايا.

3\_الليتر Letter

وهي الرسالة التي يقوم بكتابتها السبامر لإقناع الضحية , ويجب على هذه الرسالة أن تكون قوية جدا للإطاحة به في الفخ.

وهذه الخطوة يخطأ فيها مجموعة من السبامر.

4\_المايلر Miller

أهم أداة واندرها لجلب الضحايا , فبدونها لن يدخل اي شخص لصفحتك , فهو الذي يقوم بأرسال الليتل الى مئات أو آلاف البريدات الالكترونية بإيميل البايبال . وأفضل هذه الميللر هي الإنبوكس الذي يضع هذه الرسالة في انبوكس الضحية مما يرفع من امكانية الدخول اليها.

5\_الايميلات المستهدفة

وهذه الخطوة مهمة لاستهداف أصحاب البايبالات الأجنبية المليئة  , ويمكنك الحصول عليها مجانا من برامج عديدة و أهمها ميلر سبايدر.

هذه كانت أهم الأدوات التي يحتاجها السبامر , ناهيك عن الفي بي ان و الفي بي اس الذين يحمون السبامر و يسهلون عليه العملية . ]4[

ونعرض مثال لقضية اختراق أحد البنوك المصرية:

طفل مصري يخترق حسابات البنوك ويستولي على أموالها

تمكن من فك شفرات البطاقات الائتمانية.. وشراء أجهزة من مواقع التسوق**:**

**العربية.نت**

تمكنت مباحث مكافحة جرائم الأموال العامة في مصر من ضبط طالب (16 عاما) مقيم بمدينة فوة بكفر الشيخ، والمعروف بأخطر هاكرز مصري، لاستيلائه على أموال حسابات عدد من العملاء في عدد من البنوك مصرية، نظرا لخبرته الفائقة للدخول على شبكات الإنترنت وقرصنته مواقع التسوق الإلكتروني.

كان مسئولو أحد البنوك المصرية قد أبلغ الأجهزة الأمنية، عن رصده لمجهول، ينفذ العديد من عمليات الشراء لأجهزة إلكترونية وهواتف محمولة باستخدام بطاقات ائتمانية خاصة بالعديد من البنوك المصرية وغيرها لدى العديد من شركات التسوق الإلكتروني، وأن أصحاب تلك البطاقات اعترضوا على تلك العمليات لعدم قيامهم بتنفيذها، الأمر الذي أدى إلى إصابة البنك بأضرار مادية.

وتم تشكيل فريق بحث بمعرفة إدارة مكافحة الجرائم المصرفية المستحدثة، والتي توصلت إلى أن وراء ارتكاب الوقائع "محمد.س.ح"، 16 سنة، طالب تبين خلالها قيام المتهم باستغلال خبرته الفائقة في الدخول على شبكة الإنترنت وقام بالقرصنة على مواقع التسوق الإلكتروني والبنوك الأجنبية بالخارج وتمكن من سرقة بيانات البطاقات الائتمانية الخاصة بعملاء تلك المواقع والبنوك، وقام باستخدامها في إجراء عمليات شراء وتحميل قيمتها على حسابات البطاقات المستولى عليها.

وعقب تقنين الإجراءات بالتنسيق مع الأجهزة الأمنية بكفر الشيخ وإحدى شركات نقل البضائع، تم ضبط المتهم أثناء مقابلته مع مندوب الشركة بمسقط رأسه في مدينة فوه بكفر الشيخ للاتفاق معه على تسليمه عددا من الأجهزة الإلكترونية والهواتف المحمولة والتي قام المتهم بشرائها بنفس الطرق السابقة.

تم القبض عليه وبمواجهته اعترف بنشاطه الإجرامي، وأنه وراء ارتكاب الوقائع محل البلاغ وأرشد عن الأجهزة التي سبق وأن استولى عليها والتي قام بشرائها.

كما تم فحص جهاز الكمبيوتر والبريد الإلكتروني الخاص بالمتهم وتبين أنهما يحتويان على العديد من الملفات منها "فيديوهات توضح كيفية اختراق المواقع، وفك الشفرات العديد من بيانات البطاقات الائتمانية الخاصة بعملاء بنوك أجنبية، ورسائل تحوي بيانات عمليات الشراء التي قام بها المتهم على مواقع التسوق الإلكتروني المصرية وبرامج كمبيوتر للاختراق والتخفي"، وتم تحرير المحضر اللازم والتحفظ على المضبوطات وأخطرت النيابة العامة المصرية لمباشرة التحقيق.]5[

**المصادر والمراجع :**

*http://www.sama.gov.sa/ar-sa/Laws/Pages/BankingLaws.aspx*. (بلا تاريخ). تم الاسترداد من مؤسسة النقد العربي السعودي. ]1[

*http://www.arabbank.com/ar/securitystatment.aspx*. (بلا تاريخ). تم الاسترداد من البنك العربي.]2[

*https://www.riyadbank.com/ar/personal-banking/credit-cards/benefits/3d-secure*. (بلا تاريخ). تم الاسترداد من بنك الرياض .]3[

*http://th3bassma.blogspot.com/2016/04/blog-post\_10.html?m=1*. (بلا تاريخ). تم الاسترداد من عالم التقنية. ]4[

*http://www.alarabiya.net/ar/mob/arab-and-world/egypt/2015/08/29/طفل-مصري-يخترق-حسابات-البنوك-ويستولي-على-أموالها.html*. (بلا تاريخ). تم الاسترداد من العربية.]5[

**الفهرس:**

**المقدمة.................................................................................................1**

**أمن الخدمات المصرفية للبنوك على الإنترنت....................................................3**

**أنظمة لحماية البطاقات البنكية....................................................................6**

**16 نصيحة لحماية حاملي البطاقات الائتمانية من الاحتيال والسرقة.......................7**

**تعرف على السبام كي تحمي نفسك منه............................................................8**

**مثال لقضية اختراق أحد البنوك المصرية.........................................................9**

**المصادر والمراجع.....................................................................................10**

**الفهرس................................................................................................11..**