ASK PC MAGAZINE©

Free Periodical E-Publication

Supported by ASK PC Academy - Dec. 2009 - Issue No. 11

2009

THE YEAR OF THE MEGA SECURITY BREACH!

The biggest data security breaches of the year

INTRO TO COMPUTER FORENSICS

HACKING GSM

CITIBANK UNDER ATTACK

ASK PC Magazine is a FREE electronic publication published by ASK PC to enhance the information technology knowledge in Arabic language for Arabic native speakers.

ASK PC is a leading IT training company based in Egypt, UK and USA.

The opinions expressed herein are not necessarily those of ASK PC or the organizations employing the authors.
© 2009 ASK PC

ASK PC Magazine is registered at the Library of Congress.

Copying: Permission to copy for educational purposes only without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage; the ASK PC copyright notice and the title of the publication and its date appears; and notice is given that copying is by permission of ASK PC. To copy otherwise, or to republish, requires specific permission from ASK PC and may require a fee.
All names, trademarks, brands or logos mentioned here are properties of their respective owners. Certain photos and artwork used here might have special rights for their own respective owners.

ASK PC Egypt:
38 Mustafa El Nahas St., Floor 5,
Nasr City, Cairo
Egypt

Tel: +20 2 22715443

ASK PC UK:
Dalton House, 60 Windsor Avenue,
London SW19 2 RR
United Kingdom

www.ask-pc.com
www.askpc.net

From the President | كلمة الإفتتاحية

عام جديد....ولكن؟

القراء الاعزاء،

ارحب بكم جميعا في مستهل هذا العدد الجديد في ثوبه الجديد من اعداد مجلة اكاديمية ASK PC والتي يشرفنا ان نطرحها لكم ان شاءالله وبشكل دوري لزيادة المعرفة لدى القاريء العربي المهتم بتكنولوجيا المعلومات. في البداية اقدم لكم اجمل التهاني بحلول العام الجديد2010 ونتمنى ان يكون عاما سعيدا ان شاء الله عليكم جميعا وان يحقق كل انسان ما لم يستطع تحقيقه في العام 2009. لقد شهد عام 2009 العديد من الاحداث بدءا من الاحداث السياسية مرورا باحداث اقتصادية وتقنية وعلمية ولكنه في مجمله لم يكن عاما جيدا، ونحن لا نعيب على الزمان كما يقال "ولكن العيب فينا". إلا ان العام2009 في واقع الامر شهد الكثير من الاحداث المؤسفة والمزعجة والغير جيدة في اغلب الاحيان على الصعيد العالمي والإقليمي والمحلي. ومن الاحداث التي وجدنا انه من المهم ان نلفت نظر القاريء اليها، رغم ان البعض قد لا يجد هذا على علاقة بالتقنية في باديء الامر، لكن في الحقيقة لم يعد هناك شيء على هذا الكوكب او خارجه ليس له علاقة بالتقنية والعلوم. اما الموضوع فهو "الإحتباس الحراري" ومشكلات البيئة التي اثيرت في مؤتمر المناخ العالمي والتي شهدت موجه من الجدال والسجال ما بين مؤيد ومعارض "رغم شكنا فيمن يعارض" إلا ان الامر بات حقيقة لا مفر منها. الكوكب بات في خطر مما يعبث به الإنسان واصبح المناخ ايضا متغيرا بشكل ملحوظ. في الحقيقة ادهشنى ما تداوله "بعض" خبراء البيئة واساتذة الجامعات العربية والمصرية تحديدا في ان ما يتحدث عنه الغرب لهو نوع من تضخيم الامور واننا في مأمن ولا يوجد شيء كهذا ولا يجب ان نفزع البشر او نقلق "نومهم العميق" ان صح التعبير! لا يسعنا المجال هنا لسرد ما قيل تفصيلا ولكن الامر الذي يعنينا هو ان الامر بات خطيرا فعلا بغض النظر عما يقال ولا اريد البت في اننا للاسف من البلدان التي ليست في حسبان الآخرين! في عصر نجد فيه العالم مشغول باشياء لا يعير لها البشر في منطقتنا اهتماما، نجد اشياء مخجلة في مجتمعاتنا تجعلنا على قائمة الشعوب التي ستفنى "بنفسها" فهي لا تحتاج إلى ان يتدخل عدو او حبيب او صديق! فهل سيمثل العام2010 بعض التغيرات في طريقة تفكير بلداننا العربية؟ هل سنحاول الإستثمار فيما يدوم- وليس ما يهدم بالديناميت بعد انتهاء عمره الإفتراضي؟ هل سنعير القضايا الكبرى اهتماما مثل التعليم وسلامة الكوكب الذي نتقاسم هواءه المسموم؟ هل سنحاول الإستفادة من التقنية في خدمة شعوبنا بدلا من ان نصبح على قائمة الدول الاكثر استهلاكا لها في العالم بلا نتيجة تذكر؟

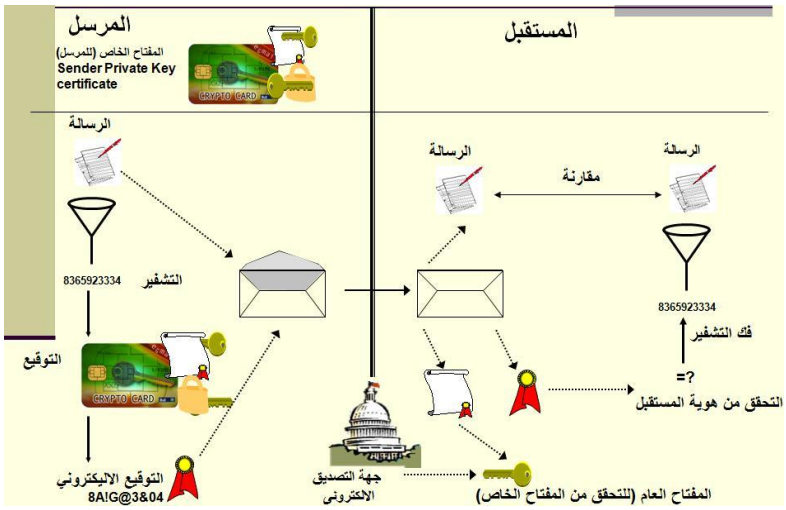
مازلت متفائلا "ولا ارى الدنيا سوداء" الامل في شبابنا، في كل من يستطيع ان يعطي، في كل من بيده بذرة فليغرسها.

لعبت علوم الحاسوب الشرعية دوراً هاماً على مدار عقود عدة بالدول المتقدمة وبالتحديد في ساحات المحاكم, وإستندت عليها بقوة في الكشف عن ملابسات جرائم عدة إرتبطت بدلائل رقمية كنظم الحاسوب, وسائل التخزين والمستندات الإليكترونية,

ولتعريف مصطلح علوم الحاسوب الشرعية Forensic Computing, فهو إستخدام علوم الحاسب الآلي للإجابة على تساؤلات تظهر بالدعاوي القضائية ويعتبر التعبير فرعاً مشتقاً من العلوم الشرعية, ولا يعتبر إستخدام تقنيات مثل التعميه والتشفير كعلوم شرعية بدون تدخل السياق القضائي.

ويفتقر عالمنا العربي بشكل موجع إلى المحققين ومحللي علوم الحاسوب الشرعية, ويعتبر هذا الإفتقار دافع المخترقين الأول للقيام بأعمال غير مشروعة حيث يسقط أهم بنود الحرص لديهم وهو الخوف من العقاب, فنادراً ما نسمع عن قضايا إليكترونية لا يتم البت فيها, وذلك لعدم الإستناد على أدلة جنائية حاسوبية وجمعها وتحليلها. بل سنجد إبتعاد معظم الدول العربية عن سن قوانين تعترف بالأدلة الجنائية الحاسوبية وعند السماح لبعض منها نجدها تُعقد شروط إستخدامها وقبولها كأدلة رقمية!

فدعونا نتذكر قصة التوقيع الإليكتروني والتي ذاع صيتها بإحدى الدول العربية منذ الزمن القريب, فقامت بمنع إعطاء الحجة القانونية للتواقيع الإليكترونية والتي يستخدم من خلالها بصمة الإصبع والأقلام والأجهزة الماسحة وسنت إصدار بطاقة ذكية معتمدة بشهادة تصديق إلكترونية صادرة من جهة مرخص لها من الهيئة المختصة بذلك وفرضت بعض الشروط والتي هي في رأيي المتواضع من الشروط التعقيدية, ودعوني أشارك حضراتكم بالمخطط الذي يشرح آلية عمل التوقيع الإليكتروني من المستند الرسمي لتلك الهئية.



(نسخة طبق الأصل من مستند هيئة تنمية صناعة تكنولوجيا المعلومات)

يوضح الرسم السابق إستخدام نظرية المفتاح المتناظر لنظم التعميهSymmetric-key Cryptosystems بشكل أساسي, وإذا تذكرنا الفتات من تلك النظريات, فهي تقوم بتشفير الرسائل.... ماذا؟ لنتوقف هنا قليلاً, ألم نبتعد قليلاً عن أصل الموضوع إلا وهو إضافة توقيع إليكتروني إلى الرسائل الرقمية؟ ناهيك عن التعقيد والتطبيق السيء الذي يظهر بالرسم, فلما تشفير الرسائل عند الحاجة إلى إضافة توقيع؟ ولماذا تم الأخذ بمصداقية تلك النظرية عوضاً عن إستخدام ما تيسر للخلق من وسائل تكنولوجيا تبسط هذه التعاقيد وفي نفس الوقت آمنة؟ ولنستكمل ما يأتي المستند على ذكره,

فهذه البطاقة تحتاج إلى عميل بريد إلكتروني واحد تقوم الهئية بتوفيره وجهاز خاص ليقوم بضبط آلياتها, عوضاً على أنه تم السماح بإستخدام التشفير على مستوى 2048 بت وهو ما كان قد تم منعه من قبل بتلك الدولة, ويستمر المستند في شرح آلية عمل التوقيع وإضافة العديد من التعاقيد والضوابط على مكان إستخدامه وتوفير أجهزة مراقبة ومصدات للسيارات وباب أمني للدخول.. إلخ!!!

وبعد توضيح أبسط الأمثلة على بعض نماذج الأدلة الجنائية الحاسوبية والتي قد يتم إستنتهاجها, نجد أن بعض الدول العربية تقوم بالفعل بتعقيد العمل على متخصصي تكنولوجيا المعلومات وعلى أنفسها, وهذا لا يعمل إلا على تأخير إمكانية ضبط العديد من المجرمين والذين هم حتى يومنا هذا طلقاء. وفيما يلي خطوات عملية جمع الأدلة الجنائية الحاسوبية:

- الوقوف على الوقائع

يتم التعرف على الدلائل الجنائية, وكيف يتم تخزينها وأين يتم تخزينها, ويقوم محلل الحاسب الجنائي بتحديد نوع البيانات المخزنة وطريقة تخزينها حتى يستطيع إختيار التقنية المناسبة لإستخلاصها.

- الحفاظ على الدليل

يتم الحفاظ على الدليل الرقمي ومحاولة عدم حدوث أي تغيير على البيانات الموجودة فيه, وهذا لا يمنع التغيير ككل للتحليل أو إستنباط المعلومات منه, ولكن يحدد هذا التغيير بأقل مستوياته.

- تحليل الدليل

يتم لإستخلاص المعلومات وتفسيرها بطريقة مفهومة إلى الأشخاص المعنية, ويتم هنا إستخدام مجموعة من التقنيات والأدوات لهذا الغرض وسنأتي على ذكرها لاحقاً.

- تقديم الدليل

ويتم هنا تقديم الدليل الجنائي إلى المحكمة وتوضيح طريقة جمعه وتحليله, وتوضيح مدى إرتباط المتهمين بالدلائل.

تقنيات جمع وتحليل الأدلة الجنائية الحاسوبية:

- على مستوى الشبكات

- التجسس على الحزم الإلكترونية Packet Sniffing

تتدفق البيانات من خلال الشبكات مثل تدفق الأوكسيجين من خلال الهواء, ويتم سحب البيانات المهمة من تلك الرزم وقد تحتوي تلك البيانات على أسماء للمستخدمين, شفرات سرية ورسائل بريدية ومن أمثلة البرامج المستخدمة لهذه التقنيات WinPcap – WPE Pro.

- تتبع عناوين الإنترنت IP Address Tracing

ويتم من خلال تلك التقنية تتبع العنوان الإلكتروني IP إلى عنوان الجهاز الحقيقي المستخدم له, وفي الحقيقة يوجد العديد من الطرق المستخدمة لتطبيق هذه التقنية ومن أمثلتها المراجعة الإرتجاعية للعناوين ويعني ذلك إحتساب أجهزة الخوادم والتي تقع بين المصدر والوجهة Source and Destination والتي يطلق عليها في بعض الأحيان "الوثبات Hops".

- تتبع البريد الإلكتروني E-mail Tracing

من المهم معرفة مصدر الرسائل الإلكترونية, ويتم ذلك من خلال تحليل عنوان البريد الإلكترونيHeader والذي يتكون بدوره من العنوان الإلكتروني للمصدر Source IP ويكشف معلومات مهمة عن خادم البريد الأصلي وبيانات وقت وتاريخ الإرسال.

1 - على مستوى نظم الحواسيب

- هيكل بنية الملفات File Structure

يتم تحليل بنية جميع الملفات المشتبه فيها, ومحاولة فك تشفير أياً منها Decryption او تصليح بعض تقنيات التشويه Garbling التي تستخدم لحماية الملفات, ويستخدم العديد من البرامج لهذه الأغراض بناءاً على اللوغاريتميات التي تم حماية الملفات بها سواء أكانت من الانواع AES – Blowfish – MD5 – Crypt – CRC أو غيرها من العديد من تقنيات الحماية المتعارف عليها.

- وسائل التخزين الرقمية Storage Media

يتم إسترجاع ما يتيسر من البيانات بإستخدام ادوات متقدمة Recovery Tools, ويتعين على الخبراء جمع هذه البيانات المبعثرة مرة أخرى لإنشاء دلائل رقمية, وقد تكون تلك الوسائل مادية ثابتة أو متحركة, وببساطة تكمن النظرية بأنه لا يوجد جهاز إلكتروني لا يقوم بتسجيل البيانات, لذلك يراجع الخبراء جميع الأجهزة الموجودة بساحات الجرائم.

- إخفاء البيانات Steganography

وهم علم أصوله قديمة وظهرت سبل تطبيقه على أمثلة عديدة, كإخفاء معلومات سرية بصورة رقمية عن طريق إستبدال بعض مكونات الصورة أو إخفاء المعلومات بداخل ملف صوتي عن طريق إستبدال بعض الأمواج الصوتية, ويعتبر هذا النوع من تقنيات الحماية من أشد التقنيات صعوبة في التتبع , ومؤخراً توفرت لدى الخبراء العديد من الأدوات التي تستند إلى طرق إرجاع المعلومات المخفية إلى نوعها الأصلي مثل سد الضوضاء بالملفات الصوتية Noise Barrage وتفريغ الحمولات المشفرة عن الملفات والصور الرقمية Encrypted Payloads

النسخ المطبوعة Print Outs

يقوم الخبراء بجمع النسخ المطبوعة التي تتوفر بساحات الجرائيم وتحليلها مايكروسكوبياً لإيجاد ما قد لا يراءى بالعين المجردة لهم, حيث تقنيات للخداع Deception تقوم بدمج بيانات مشفرة أو مشوهة ببيانات أصلية.

فدائماً ما يستند خبراء الدلائل الجنائية الحاسوبية على تقنيات وأدوات أساسية لا تخلو حقائبهم الإلكترونية منها, وذلك للوقوف على معظم وسائل الحماية والتشويه التي تتعرض لها البيانات الرقمية, ولعل أكثر الأمثلة لتلك التقنيات المستخدمة من قبل الخبراء, محررات الشيفرات Hex Editors - أدوات التحليل Disassembles – أدوات فك التشفير Decryptions – أدوات نظم عنواين النطاقات DNS

ومن الواجب التوضيح بأن خبراء الدلائل الجنائية ليسوا رجال قضاء أو محامين, ولا يحتاج هؤلاء إلى أن يتعلموا علوم القانون ويمارسوا وظيفة قانونية معينة لذلك, بل تمكنهم دراسات علوم الدلائل الجنائية من إكتساب المعلومات القانونية الكافية لإستخدامها في عملهم وقد يكونوا متخصصين في تكنولوجيا المعلومات أو أمن المعلومات, وهناك إعتقاد خاطيء نراه بالمجتمع العربي وهو ضرورة توظيف هؤلاء الأشخاص بالهيئات الأمنية الحكومية أو إشتراط تعيينهم رجال شرطة حتى يعترف بهم القضاء, وهذا فهم خاطيء لطبيعة خبرات هؤلاء الأشخاص حيث تلعب السمعة المهنية والأمانة الدور الأول في تحديد مدى مصدقياتهم والإعتراف بهم.

وللبدأ بسد فجوات الإفتقار العربي لعلم الدلائل الجنائية الحاسوبية, يقع عاتق كبير على كلتا الأطراف المعنية من حكومات ومنظمات تجارية, فعلى الحكومات العربية سن قوانين خاصة بالجرائيم الإليكترونية وتحديد معايير ضبط الإستخدام الالكتروني وما قد ينتج عنه من منافع أضرار تقع على الأفراد والمؤسسات والإقتصاد القومي ككل, فقد أشارت شركة محاربة الفايروسات ترينـد مايكرو إلة وجود أكثر من 700 ألف حالة إنهيار نظامي خلال تسمعة شهور فقط في دول عربية متقدمة مثل السعودية والإمارات العربية المتحدة حيث بلغت نسبب التضرر إلى 64% و20% بالنسبة للأخيرة, وبناناً على سن قوانين مكافحة للجرائم الإلكترونية سيتعين على الحكومات تعيين مستشارين للدلائل الجنائية الحاسوبية والإهتمام بدورهم.

أما بالنسبة لدور المؤسسات التجارية فعليها بأخذ الحذر حتى لا تقع تحت قبضة القانون سواء عن قصد أو دون أن تدري! فعليهم الإهتمام بدور القانون وتأثيره على نشاطها التجاري وتحديد قائمة بخبراء شرعيين في التكنولوجيا للإستعانة بهم لاحقاً في حالة إحتياج خبراتهم بالمسائل التي تستطلب عناية حرجة للمشاريع,

الخاتمة

يغطي علم الدلائل الجنائية الحاسوبية عمليات تحليل نظم الحاسوب لإستخدامه في الوسائل الشرعية, وعلى المؤسسات الحكومية والتجارية مراعاة دمج أنشطتها بالقانون طالما تدخلت الأعمال الإليكترونية, لطالما أزعجنا تدخل التعقيد في حل مشاكلنا المعقدة في الأساس! نأمل من السادة القراء أياً كانت طبيعة أعمالهم الأخذ بالمبادرة والتفحص في الموضوع فلن ينهض بأمتنا العربية إلا خير جيلها.

بقلم: عمرو موسى

admin@amromoussa.net

ASK PC

تخصصات معتمدة عالميا في تكنولوجيا المعلومات...
شهادات معتمدة عالميا...

لكل من يبحث عن التميز في تكنولوجيا المعلومات والإتصالات

BCS
REGISTERED COURSE PROVIDER

IEEE

ISSA™
Information Systems Security Association
The Global Voice of the Information Security Profession

BRITISH INSTITUTE FOR LEARNING & DEVELOPMENT
ORGANISATIONAL MEMBER

Your Career starts here!

Internationally recognized IT qualifications
Vocational & Academic Programs
eLearning & Instructor-led Training

ASK PC in Egypt:
38 Mustafa El Nahas Street,
Floor 5, Nasr City, Cairo

+20 2 22715443
+20 12 4473366

www.ask-pc.com
www.askpc.net
info@ask-pc.com

عام 2009 عام اختراقات امن المعلومات من العيار الثقيل

شهد عام 2009 العديد من الإختراقات الامنية المتعلقة بتقنية المعلومات التي استهدفت جميع القطاعات العالمية والمحلية والإقليمية والتي طالت حتى اختراقات في الامن العام لدول كبرى! وتشير الإحصائيات المختلفة والابحاث والمصادر العلمية ان العام 2009 هو عام الإختراقات الاكبر على الإطلاق. وسوف نلقي نظرة عن كثب في هذا المقال عن اهم الإختراقات والمشكلات الامنية التي بالفعل قد تجعل من عام 2009 عام الإختراقات الاكبر على الإطلاق.

ولكن قبل ان نبدأ في سر هذه الاحداث، لابد ان يعلم القاريء العزيز ان الحرب ما بين المخترقون وخبراء امن المعلومات لن تنتهي رغم كل محاولات الخبراء للتقليل من الهجمات والحد من هذه الإختراقات إلا انها في تزايد على عكس ما يتوقع الخبراء. فكما تتيح التقنية الكثير من الادوات للخبراء لتحليل وحماية البيانات والحد من الهجمات فهي ايضا تتيح للمخترقين اكثر بكثير من هذا وربما جعلت عملهم اسهل بكثير من ذي قبل! وهذا ادعى إلى الإهتمام بعلم كعلم امن نظم المعلومات اكثر من ذي قبل وان الحاجة إلى خبراء في هذا المجال سوف تظل متزايدة على جميع الاصعدة سواء في القطاعات الحكومية او الخاصة او على الصعيد الشخصي. إلا ان الخبراء المطلوبون في هذا النوع من التصدي للجرائم الإليكترونية يصعب ان تجدهم. ولعل هذا الخبر الذي ادلى به مسؤلون في امن المعلومات في الحكومة الامريكية في صحيفة الواشنطن بوست، من ان الامر بات صعبا والحاجة إلى هؤلاء الخبراء اصبحت ضرورة من ضروريات العمل وليست رفاهية رغم صعوبة ايجادهم للكثير من الاسباب.

واليكم فيما يلي اهم هذه الاحداث التي تعتبر صفحة لتقدم تقنيات امن المعلومات في العام2009

Malicious Code -

استطاع المخترقون في هذه العملية اختراق احد اشهر الشركات في مجال تسجيل اسماء النطقاقات والإستضافةHosting وقاموا بزرع كود خبيث Malicious Code في الكثير من المواقع ادت هذه الاكواد التي ظلت لمدة3 اشهر، إلى سرقة اكثر من 573000 بطاقة ائتمان. من المعروف ان اختراقات المواقع باتت خطرا كبيرا وتشير الإحصائيات بان 70% من المواقع الموجودة على الإنترنت قابلة للإختراق!

- اختراق بريد المدير

احدى اكبر شركات البريد الإليكتروني، عرضت جائزة قدرها10000 دولار لمن يستطيع ان يخترق البريد الإليكتروني الخاص بمدير الشركة. ظنا منها ان ما تستخدمه من انظمة حماية لا يستهان بها، وعلى العكس جاءت الرياح بما لا تشتهي السفن، وتم اختراق البريد الإليكتروني بثغرة من ثغرات المواقع المعروفة باسم XSS

- بريد ملغم من صديق

في حادثة تعد من اكثر الاحداث مدعاة للسخرية إلا انها تسببت في خسارة فادحة لمستشفى شهر. قام احد الشباب على علاقة بفتاة تعمل في هذه المستشفى بارسال رسالة بريد اليكتروني بها برنامج تجسس Spyware ليعرف ماذا تفعل. وبالفعل قامت

الفتاة بفتح الرسالة وتم تشغل البرنامج الذي ادى فيما بعد إلى استخدام مخترقون آخرون لهذا البرنامج للحصول على معلومات هامة من المستشفى. وهذا يدل على عدم الوعي في هذه الجهات لامن المعلومات.

- اختراق وسائل الإعلام

لقد ظهرت في العام 2009 اكثر من غيره من الاعوام ما يعرف بمصطلح Macking او Media Hacking حيث استطاع الهاكرز استخدام مواقع مثل Twitter في عمل هجمات على بنى تحتية في بلدان باكملها وفي وجود هذه التقنيات في هذا العصر الذي تستطيع ان ترسل ملايين الرسائل في وقت قصير فإنه بالامكان تجنيد هذه التقنيات لنشر ملايين الديدان والبرمجيات الخبيثة ايضا وهذا تحدي جديد لخبراء امن المعلومات.

- الموظفون الخطر الاكبر

يعتبر العام 2009 عام اختراقات الموظفين. حيث ان العاملين في الشركات والمؤسسات من اضعف النقاط التي يمكن التسلل عبرها إلى بيانات حساسة دون عناء كبير. والامثلة كثيرة منها احد موظفي شركة من شركات الإتصالات كان يعمل بشكل مؤقت في الشركة واستطاع ان يحصل على بيانات شخصية للعملاء مكنته من سرقة ما يقرب من 70000 دولار من حساباتهم في فترة وجيزة. وحتى احدى اشهر الشركات العاملة في مجال امن المعلومات وانتاج برمجيات مكافحة الفيروسات ضبط لديها موظف يقوم بسرقة بطاقات الإئتمان الخاصة بالعملاء. ويبدو ان هذه المشكلات لن تنتهي وسوف تستمر معنا في العام2010

- جامعة كاليفورنيا

في واحدة من اعرق الجامعات في الولايات المتحدة تم اختراق قاعدة بيانات للخريجين وتم اتاحة بيانات اكثر من160000 شخص على الإنترنت وظلت متاحة طيلة 6 اشهر دون ان يشهر المسؤلون!

- Google

حتى جوجل اكبر الشركات العاملة في مجال الإنترنت والتقنية لم تسلم في العام2009 من اختراقات في امن المعلومات حيث تعرض البريد Gmail وشبكة Adwords والعديد من تطبيقاتها للإختراق. وتعتبر جوجل من اكثر الشركات ايضا تعرضا للهجمات من قبل المخترقين فهي هدف دائم لهم.

- بطاقات الإئتمان

من اكثر الاحداث التي اثارت جدلا كبيرا في الولايات المتحدة في تمكن احد المخترقين من سرقة130 مليون بطاقة ائتمان من اشهر الشركات التي تعمل في بطاقات الإئتمان مما ادى إلى خسائر فادة ايضا على صعيد العديد من البنوك المتعاملة مع هذه الشركة وتعتبر هذه العملية من احدى اشهر عمليات سرقة الهوية ID Theft في العالم.

- المنطقة العربية

لم تسلم المنطقة العربية من اختراقات امن المعلومات والجرائم الإليكترونية التي تنامت في العام2009 عن ذي قبله وهذا احد اهم المؤشرات التي تحدثنا عنها في بحثنا عن الجريمة الإليكترونية في الشرق الاوسط وانها آخذة في ازدياد لا محالة لاسباب كثيرة ذكرت في البحث المنشور عام 2008! ولعل اشهر هذه الحوادث التي حدثت في مصر والتي تؤكد ان الجريمة الإليكترونية لا تعرف حدودا هي عملية سرقة اموال بعض عملاء من بنوك اجنبيه واطلقت عليها FBI عملية Operation Phish Phry إلا انه لغياب القوانين والوعي والخبرات، فهذا النوع من الجرائم من الصعب التعامل معه في منطقتنا للاسف.

- اختراقات الامن القومي

في العدد التاسع من المجلة اشرنا إلى موضوع هام وهو اختراق الامن القومي Hacking National Security ولقد كان للولايات المتحدة نصيب الاسد في هذه الاختراقات في العام 2009 بدءا من اختراق شبكة الكهرباء حتى شرقة مخططات الطائرات الحربية والوثائق السرية. ونكاد نجم بان العديد من الدول ايضا قد عانت من هذه الإختراقات ومازالت تعاني إلا ان غياب الشفافية وعدم الإفصاح عن كل ما يحدث يجعل التحقق من هذه الاحداث ليس عملية هينة في مثل هذه البلدان والتي منها بلداننا.

- مصادر هامة لإختراقات العام 2009

http://www.forbes.com/2009/11/24/security-hackers-data-technology-cio-network-breaches.html

http://www.bankinfosecurity.com/articles.php?art_id=1766

http://techbuddha.wordpress.com/2009/01/20/2009-the-year-of-the-largest-security-incidents-/since-the-beginning-of-forever

http://www.breach.com/resources/whitepapers/downloads/WP_TheWebHackingIncidents-2009.pdf

http://www.lifedork.net/more-facebook-xss-hacking-2009.html

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

http://www.chtlj.org/sites/default/files/media/articles/v025/v025.i2.Peretti.pdf

http://www.thermcadvisors.com/ITRC%20Breach%20Stats%20Report%202009.pdf

http://www.thermcadvisors.com/ITRC_Breach_Report_20090930_1.pdf

د. محمد الجندي

فيرس ال Facebook , قد يجند جهازك لتدمير أجهزة أخري

جعلوني مجرماً , قد تصلح هذه المقولة عنواناً لأحد الأفلام , و لكنها أيضاً قد تصلح عنواناً لموضوعنا اليوم .

لقد كان هناك فيرس , او بمعني أصح دودة Worm , منتشرة علي ال Facebook , و أيضاً قد قامت بضرب مواقع أخري مثل MY Space , Google , و هذه ال Worm , تسمي Koobface , و لقد كانت هذه ال Worm , تقوم بعملها بالطريقة الأتية :-

انه بموقع ال Facebook يتم أرسال تنويهات بخصوص الفيديوهات , او الصور التي يقوم أحد أصدقائك , بالأشارة إليك فيها من خلال ال TAG , فيتم أرسال تنويه لك بذلك في حسابك , علي ال Facebook , و أيضاً علي الأيميل الخاص بك .

فلقد قامت ال Worm , بأستغلال ذلك , من خلال القيام بأرسال تنويهات مزيفة , مضمون هذه التنويهات أن احد اصدقائك قام برفع فيديوا , انت فيه , او موقف محرج حدث لك , فتكون عنوانين هذه الرسائل غريبة , بحيث يثير فضول الشخص لكي يضغط علي اللينك , لرؤية هذا الفيديو , و في الغالب تكون عنوانين هذه الرسائل كالأتي :-

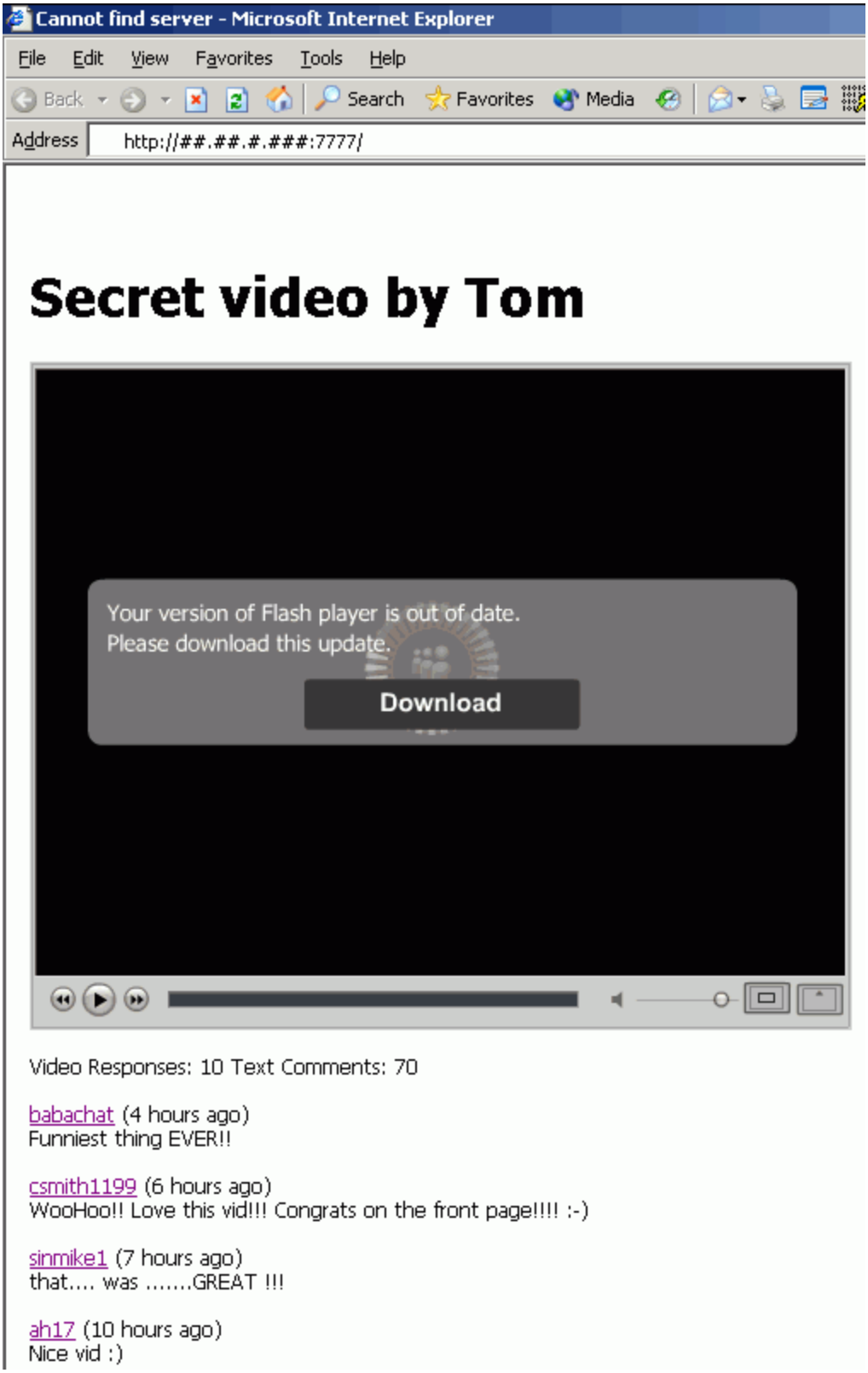
Hey, I have this hilarious video of you dancing

You should check it out .Your face is *so red* .

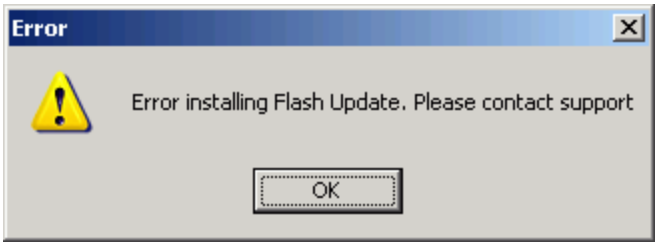
فعندما تقوم بالضغط علي اللينك الخاص بالفيديو , يتم تحويلك إليه بالفعل بطريقة عادية جداً , و لكن الخدعة تكمن في , انه عندما تقوم بتشغيل الفيديو سوف تظهر لك رسالة تخبرك : بأنك يجب ان تقوم بتحديث ال Flash Player , و يقوم بإظهار

كلمة Download , لكي تقوم بالضغط عليها , و تحميل الـFlash Player.exe

و الخدعة تكمن في أن ما تقوم بتحميله علي جهازك ليسFlash Player.exe, بالفعل , و لكنه يقوم بتحميل Trojan , تحت اسم tiny proxy.exe.



فعندما تقوم بعمل Download , و القيام بتنصيب البرنامج , تظهر لك رسالة خطأ مزيفة ثم يبدأ ال Trojan بالعمل .



حيث يقوم بداية بسرقة الباسورد الخاص بك , و بعض المعلومات الاخري , و يكون جاهزاً لمهاجمة أي جهاز اخر , أو اي موقع أخر , و أيضاً يكون جهازاً للقيام بعمل Download لبرامج اخري , أو Trojans أخرين .

و بهذا يكون قد شارك جهازك , في عمليات تخريبية , أو هكر علي مواقع أو اجهزة أخري دون , ان تدري , و في النهاية يمكن ان تقول (جعلوني مجرماً) .

وهذا هو تقرير شركة الحماية Kaspersky عن Koobface

http://www.kaspersky.com/news?id=207575670

و هذه هي النصاح التي ينصح بها موقع ال Facebook , للمصابين بهذا الفيرس .

http://www.facebook.com/security

و تدور هذه النصائح حول , انه يجب تغيير الباسورد الخاص بالحساب الخاص بك علي ال Facebook , بمجرد أن تعلم انه تم أرسال Spam من خلال الأكونت الخاص بك , و أيضاً تتضمن بعض النصائح حول عمل أسكان علي جهازك من خلال أنتي فيرس , او من خلال بعض المواقع الخاصة بعمل الاونلاين اسكان .

و في الغلب اي برنامج انتي فيرس يتم تحديثه , سوف يتعرف علي هذا الفيرس , و كذلك أيضا الأداة الخاصة بمايكروسوفت الخاصة بأزالة البرامج الخبيثة , و التي يمكن تحميلها من خلال هذا الرابط .

http://www.microsoft.com/downloads/details.aspx?FamilyId=75B8EB14-9AB3-4F54-E72D-AD724AE0&displaylang=en

- و كل ما سبق ذكره يجعلنا نتعرض لمصطلح دارج في مجال أمن المعلومات , و هو Zombie Computers

معني كلمة Zombie , هي العائد من الموت , و قصة ال Zombie , معروضة في ال Games , و الأفلام , علي انهم جماعة من الناس , اموات , ولكنهم رجعوا الي الحياة , و ذلك نتيجة فيرس , انتشر بينهم , فأصبحوا الأموات الأحياء , و يقومون بنشر

هذا الفيرس بين كل من يتعرض للعض منهم .

فهي نفس الفكرة , في اجهزة الكمبيوتر , حيث يقوم الجهاز الZombieبأصابة أجهزة , أخري , و يتم التحكم فيها تحكم كامل , و يقوم الهاكر بسرقة كلمات السر , و أرقام الفيزا , و أيضاً , يقوم بأستخدام هذه الاجهزة , لأرسالSpam , و كذلك يستهدف بها مواقع أخري .

و يمكنكم التعرف اكتر عن Zombie Computers من هنا :-

http://en.wikipedia.org/wiki/Zombie_computer

و النصيح الأولي , و الأخيرة , لكي تحمي نفسك من أن يكون جهازكZombie , دون ان تدري , ان تتابع دوماً التحديثات التي تصدرها شركات أنظمة التشغيل , و أيضاً ان تهتم بالحماية الخاصة بالجهاز , من خلال تنصيب برنامج حماية , و تحديثه دوماً .

بقلم / محمد عماد

Emad_emmbk@hotmail.com

Hacking GSM

الهواتف النقالة او الهواتف المحمولة او الجوال. اختلفت المسميات والغرض واحد. في سابقة ايضا للعام2009 تمكن احد الخبراء الالمان من فك تشفير النظام الخاص بالإتصالات عبر الهواتف النقالة GSM مشيرا إلا ان ملايين البشر حول العالم في خطر نظرا لضعف الانظمة المستخدمة في التشفير.

ورغم رفض مجموعة GSM الإعتراف بهذا الامر إلا ان الخبير الالماني الذي يدعى Karsten Nohl عرض هذا الامر في مؤتمر في برلين واشار إلى ان عمله قانونيا وهو قام بهذا من الناحية العلمية لتأكيد ان الانظمة المستخدمة في تشفير الإتصالات الرقمية للهواتف المحمولة غير كاف لحماية خصوصية المستخدمين ومعرض للإختراق.

وللأسف الشديد فأن هذه الخوارزمية المستخدمة في التشفير تستخدم في اكثر من 80% في انظمة الهواتف المجمولة حول العالم! وهذا سوف يجعل الامر اكثر تعقيدا على جميع الاصعدة. ورغم فداحة وخطر هذا الامر إلا ان الخبراء ليسوا واثقين من ان مجموعة GSM سوف تتبنى نظاما جديدا في الفترة الحالية لكثير من الإعتبارات اهمها الإعتبارات الإقتصادية تاركة الملايين مهددين باختراق خصوصيتهم.

للمزيد: http://www.nytimes.com/2009/12/29/technology/29hack.html?_r=2&ref=technology

Citibank under Attack

لم تسلم مجموعة سيتي جروب المالكة لسيتي بنك من مشكلات اقتصادية جراء الازمة المالية في العام 2009 فحسب إلا انها ايضا تعرضت إلى العديد من الإختراقات على صعيد امن المعلومات والتي طالت الكثير من الحسابات وادت إلى سرقة ارصدة كبيرة تقدر بعشرات الملايين من الدولارات طبقا لتحقيقات FBI وقابلت مجموعة سيتي جروب هذا الامر بالنفي رغم انها اعترفت باختراقات في انظمة الحسابات الخاصة بها. إلا ان المباحث الفيدرالية لديها ادلة من جراء القبض على مجموعة من شبكة للجريمة الإليكترونية المنظمة من روسيا تشير هذه الادلة إلى صحة الإدعاءات بضياع هذه المبالغ فعلا من ارصدة العملاء التي حاولت سيتي جروب التستر عليها وتغطية بعضها بالخسارة!

وهذا ما اشار اليه احد المتضررين فعليا في الحادث حيث سرق من حسابه اكثر من مليون دولار قامت سيتي بنك بتغطية80% منها مرة اخرى لهذا الرجل!

للمزيد: http://www.scmagazineus.com/citibank-refutes-reported-hack-by-russian-gang/article/160124/

الحكومة الإليكترونية او كما يشار اليها باللغة الإنجليزية E-government أو eGOV هو نظام حديث تتبناه الحكومات باستخدام الشبكة العنكبوتية العالمية والإنترنت في ربط مؤسساتها بعضها ببعض، وربط مختلف خدماتها بالمؤسسات الخاصة والجمهور عموماً، ووضع المعلومة في متناول الأفراد وذلك لخلق علاقة شفافة تتصف بالسرعة والدقة تهدف للارتقاء بجودة الأداء. و يعتقد أن أول استخدام لمصطلح "الحكومة الإلكترونية" قد ورد في خطاب الرئيس الأمريكي بيل كلينتون عام 1992.

وفي العام 2002 عرفت الأمم المتحدة الحكومة الالكترونية بأنها "استخدام الإنترنت والشبكة العالمية لتقديم معلومات وخدمات الحكومة للمواطنين". وقدمت منظمة التعاون والتنمية في المجال الاقتصادي (OECD) في عام 2003، التعريف التالي "الحكومة الإلكترونية هي استخدام تكنولوجيا المعلومات والاتصالات وخصوصاً الإنترنت للوصول إلى حكومات أفضل". وهناك أيضاً تعريفات أخرى لعدد من الباحثين في مجال الحكومة الالكترونية فمنهم من عرفها بأنها وسيلة لتحسين القطاع العام والحكومي وآخرون ركزوا على جانب تحسين الاتصال مع المواطن وتحقيق ديموقراطية أكبروالبعض ذكر انها مسألة تجارية تتعلق بزيادة العوائد وتحسين الأداء والوضع التنافسي للهيئات والدوائر الحكومية.

طبيعة الخدمة المقدمة عبر الحكومة الإليكترونية:

تشير الدراسات إلى ان اغلب الخدمات التى توفرها الحكومة الإليكترونية تندرج تحت احدى التصنيفات التالية:

- **علاقة الحكومة بالمواطن او العميل**
- **علاقة الحكومة بقطاع الاعمال**
- **علاقة مؤسسات الحكومة بعضها ببعض**
- **علاقة الحكومة بموظفيها**
- **وهناك علاقة اخرى قد لا تتوفر على الملأ وهي الاجهزة الإليكترونية المستخدمة من قبل الحكومات في اطار داخلي وتشمل الإتصالات والاجهزة التقنية مثل اجهزة الأمن المرتبطة بشبكات مركزية فهي ليست متاحة للجميع**

أهداف الحكومة الإلكترونية

تدعم الحكومة الإلكترونية عمليات الحكومة الكلاسيكية من حيث تقديم الخدمات آلياً لجمهور المستفيدين ومشاركتهم في صنع القرار وصولاً إلى تحقيق شفافية أكثر في عملية الحكم، كما تهدف إلى تخفيف الأعباء المالية في الإدارات العامة لجهة كلفة إجراء الخدمات مع المحافظة على مستويات عالية لجودة الخدمات، وبما أن الحكومة الإلكترونية سوف تستهدف مجموعات مختلفة من المستفيدين كان من الممكن أن نقدم الأهداف الإلكترو-حكومية حسب المجالات التالية:

• المجال الحكومي- الشعبي: في مجال علاقة الحكومة بمواطنيها، سوف تقع معظم أهداف الحكومة الإلكترونية في خانة رفاهية المواطن ومشاركته في الحكم، ففي الهدف الإستراتيجي الأول تستطيع الحكومة توصيل الخدمة إلى المواطن بدلاً من أن يصل هو إليها وذلك بإستخدام تكنولوجيا الإنترنت والإتصالات، بينما تساعد أنظمة الحكومة الإلكترونية في مجال التصويت الإلكتروني والإنتخابات الإلكترونية على توسيع دائرة المشاركة الشعبية في العملية الديموقراطية.

• المجال الحكومي – المؤسساتي: تهدف الحكومة الإلكترونية في هذا المجال إلى تنشيط الدورة الإقتصادية عبر تسهيل معاملات المؤسسات التجارية سواءً كانت مؤسسات محلية، إقليمية أو عالمية.

• المجال الحكومي – الحكومي: على المستوى الحكومي الداخلي، سوف يكون في صميم أهداف الحكومة الإلكترونية الهدف الرامي إلى ردم الفجوة البيانية والإجرائية بين مختلف الوزارات والإدارات العامة، بالإضافة إلى رفع مستويات الكفاءة والفعالية والأداء في الإجراءات والأنظمة الحكومية الداخلية من قبيل مكننة جميع الادارات العامة على سبيل المثال.

• المجال الحكومي – الخارجي: من أهم أهداف الحكومة الإلكترونية في هذا المجال هو عملية دمج الحكومة بطريقة انسيابية وذات جدوى إقتصادية مع محيطها الخارجي، ومن الممكن أن نعدد بعض الأهداف التفصيلية مثل تشجيع السياحة عبر تقديم خدمات ومعلومات سياحية عن البلد للمؤسسات السياحية الخارجية أو للمواطنين الأجانب، كما يعتبر تشجيع الاستثمار الخارجي أحد الأهداف التفصيلية في هذا المجال.

كما رأينا فإن الحكومة الإلكترونية تسعى من خلال نموذجها الجديد أن تساهم في رفد الاقتصاد الوطني وتحسين صورة البلد بشكل عام بالاضافة إلى خدمة العنصر الأهم في المجتمع ألا وهو المواطن.

وعلى الرغم من كون الباحثون يشيرون إلى ان الحكومات الإليكترونية سوف تخلق لونا جديدا من الشفافية مع المواطن على الاقل وايضا نوعا من الحرية في التعبير عن الراي وما إلى ذلك إلا ان البعض الآخر من الخبراء لا يرون ذلك لانهم يرون انها تدار بنفس الآليات والبروقراطيات التي تدار بها الحكومة الغير اليكترونية ناهيك عن مشكلات العمالة الغير مدربة وتحديث او نقل او حذف البيانات من المواقع الحكومية دون اشعارات مسبقة وبدون اسباب وجيهة كالتي حدثت في الولايات المتحدة بعد تفجير 11 سبتمبر حيث حذفت الحكومة الامريكية الكثير من المعلومات من مواقع الحكومة الإليكترونية تحت مسمى الأمن القومي!

فوائد الحكومة الإليكترونية:

الفائدة الاساسية من خمات الحكومة الإليكترونية هو تقديم خدمات الحكومة العادية للمواطن على الإنرنت للمساهمة في تقليل الاعباء على المواطن وتضييع الوقت والجهد والمال وايضا تعود على الحكومة بالمزيد من الإدارة والترتيب للخدمات والسرعة في انجاز المهام وتقليل البيروقراطية.

للمزيد عن الحكومة الإليكترونية زالخدمات والفوائد والحوكمة:

http://www.egovconcepts.com

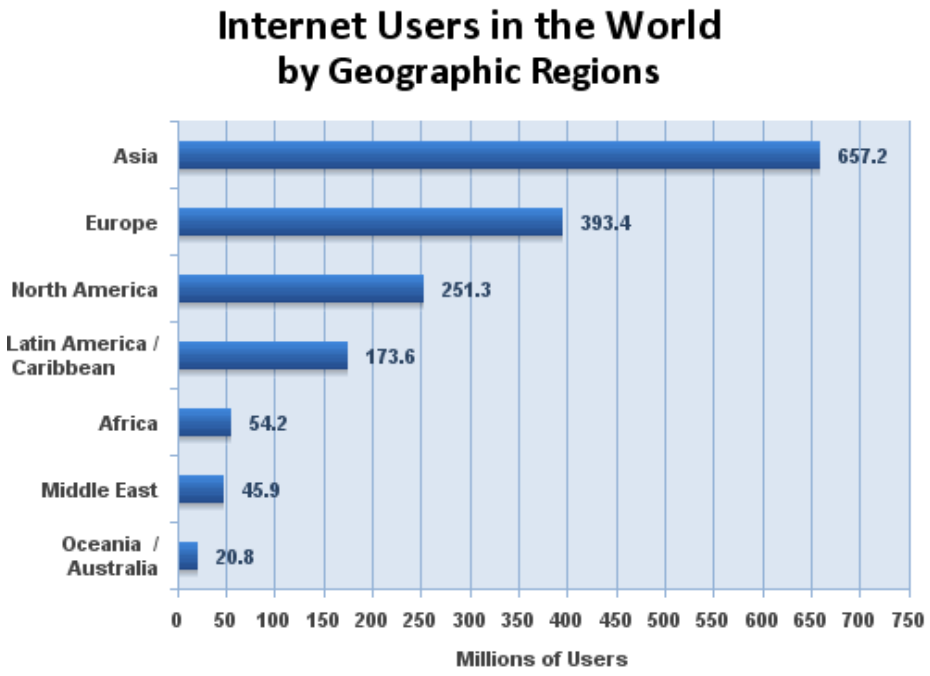
د. محمد الجندي

مما لاشك فيه ان الإنسان بطبيعته يميل إلى التغيير وان الثقافة البشرية تتغير عبر الزمن بشكل واضح ولكن لم يغير البشرية بهذا الشكل وبهذه السرعة شيء مثل الإنترنت فقد اثر حتى في طريقة التفكير والسلوك والمجتمع بشكل كبير في خلال فترة لا تعدو العقدين. وهذا يدل على الاثر الكبير للإنترنت في المجتمعات وتشكيل الثقافات.

وطبقا للإحصائيات العالمية فان عدد مستخدمي الإنترنت يزداد زيادة كبيرة كل عام عن ذي قبل فعلى سبيل المثال يشير موقع الإحصائيات الشهير Internet World Stats إلى ان اسستخدام الإنترنت في العالم قد وصل إلى23.8% من نسبة تعداد شكان العالم وهي نسبة كبيرة في فترة قصيرة حيث ازداد عدد المستخدمين منذ 2000 إلى 2008 بنسبة 342.2% ويمثل الشكل التالي عدد المستخدمين حول العالم بالمليون

وتمثل اسيا اكبر نسبة من المستخدمين نظرا لعدد السكان ووجود الصين!

وهذا العدد من المستخدمين بالطبع يستخدم الخدمات التي تقدمها الإنترنت من بريد اليكتروني ووسائط متعددة ومحتوى



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Estimated Internet users are 1,596,270,108 for March 31, 2009
Copyright © 2009, Miniwatts Marketing Group

اليكتروني وترفيه واخبار وتجارة وما هو اكثر من ذلك حيث خلق عالما افتراضيا جديدا بمعايير ومواصفات خاصة.

واشار بيل جيتس "ان الإنترنت سيكون محور التركيز للشركات والافراد والحكومات على حد سواء"

ولقد فرض الإنترنت ثقافات جديدة نتاج تقنيات وصناعات جديدة لم تكن موجودة من قبل حيث اصبح الإنترنت ظاهرة ثقافية عالمية. وقد اثرت بالفعل في حياتنا وفي نمط تفكيرنا ورؤيتنا للامور وغيرت في ثقافاتنا.

ومن المعروف ان الإنسان تتغير ثقافته وطرقة تفكيرة بالتفاعل والتواصل مع الآخرين وهذا ما وفره الإنترنت بسهولة بين هذا العدد الهائل من المستخدمين حول العالم. حيث خلق بيئة اجتماعية جديدة تفرض قوانينها وشروطها على كل من يتعامل معها. فقد اثر الإنترنت في الحياة اليومية للفرد الذي هو جزء من المجتمع سواء كان هذا المجتمع صغير او كبير حيث تغيرت طرق

اداء المهام وغيرت نمط الحياة وكيفية التعامل مع الاعمال والامور الحياتية الاخرى. وبما ان هذا الفرد جزءا من منظومة اكبر هي المجتمع فكان من الطبيعي ان ينقل هذا الفرد ما تاثر به إلى المجتمع الذي ينتمي اليه.

ومن احد اشهر الاشياء التي تغيرت في ثقافات المجتمعات هي احترام القوانين والخصوصية والملكية الفكرية فقد ادى انمتشار الإنترنت والمحتوى في كل مكان حتى في الهاوتف النقالة إلى تغير سلوك الفرد والمجتمع فعلى سبيل المثال كانت السرقة دائما شيئا منبوذا وغير محبذ ويعاقب عليه القانون في المجتمع ولكنك ترى الفرد الآن على الإنترنت لا يأبه لتحميل آلاف الاغاني والكتب المقرصنة والمسروقة غير آخذ في اعتباره ان هذه سرقة... وتعدي على حقوق الغير!

ومن بعض السلوكيات الاخرى التي تغيرت في الفرد وبدأت تظهر بصورة تصل غلى حد الإدمان في المجتمع ككل "عادة قراءة البريد الإليكتروني" التي اصبحت عادة لا يستطيع كل من يتعامل مع الإنترنت اغفالها او اعهمالها كليا او جزئيا فاصبحت جزءا من السلوك اليومي للفرد والمجتمع على السواء.

ومن احد اشهر الامثلة الاخرى لتغير سلوك البشر وهو "تغير سلوك الفرد في تلبية رغباته" حيث اصبح من السهل تلبية الحاجة إلى الحب والإنتماء إلى مجتمع ما عن طريق غرف الحوار والدردشة والإنخراط في المجتمعات الإفتراضية.

واصبح الإنترنت ايضا ساحة لتلبية احتياجات الفرد من التعليم والإحساس بالأمان وايضا سهولة الوصول إلى الاعمال وتلبيات مختلف الإحتياجات بطرق اسهل واسرع من ذي قبل حتى ان الامر وصل إلى الغذاء. فبدات الثقافة تتغير وبدات تنتقل ثقافات ربما كانت غير معروفة من قبل إلى ثقافات اخرى اكبر وربما اثرت الثقافات الصغيرة في الثقافات الاكبر نظرا لوجودها الكبير على شبكة الإنترنت مثل ازمة المحتوى العربي على الإنترنت والمقابل من اللغات الاخرى على سبيل المثال لا الحصر...

واثر الإنترنت على الثقافة ايضا حيث غير طرق التفكير حيث اصبحت على سبيل المثال القرارات الجماعية اسهل واسرع واكثر تأثيرا عن ذي قبل بفضل توفر تقنيات مثل المؤتمرات الإفتراضية والفيدو والدردشة والإتصالات عبر الإنترنت بشكل عام.

وذهبت ثقافة الإنترنت إلى ما هو ابعد من ذلك حيث بدات تأخذ منحى التأثير كصوت مسموع في بعض البلدان التي تقلص حرية الفرد في المجتمع او الحياة السياسة وما شابهها من ادوار يفتقدها الفرد في مجتمعه يعيش فيه فأصبح الإنترنت البوق الذي يتحدث به دون ان يتعرض للمشكلات رغم ان هذا لم يكن متوقعا في بعض البلدان إلا انه اصبح واقعا مؤثرا لدرجة ان مواقع بعينها مثل Facebook و YouTube قد نقلت ثقافات وافكار وقرارات وسياسات بغض النظر عن ما ورائها من نية إلى مناطق اخرى من العالم عبر الإنترنت ورسمت صورا ربما تكون قد شوهت الحقيقة او ربما تكون قد عرت الحقيقة في بعض الاحيان!

فبلد مثل الصين استخدمت فيه الإنترنت في بدايات العام 2000 للتغلب على تقييد حرية النشر وتعرية الحقائق السايسة الغائبة عن المجتمع وادنة للحكومة! وهذا مثال تكرر بعذد ذلك مرارا وتكرارا ربما يكون واضحا في الدول المتقدمة والدور العربية ايضا على السواء ولعل ابرز هذه الظواهر ظاهرة المدونات التي كان لها اثرا بالغا في تغيير الثقافة لدى المجتمع وتحول اكثر الشاب إلى التدوين في فترة من الفترات قبل اتجاههم إلى التجمعات الإفتراضية مثلFacebook

ورغم ان العالم قد انفتح على ارجائه عند ظهور القناوات الفضائية والبث الفضائي المفتوح وبدأت الثقافة تتغير ولم يعد من اسهل تضليل الحقيقة واخفائها عن اعين المجتمع الذي قد يبحث عنها او حتى بدون ان يبحث عنها إلا ان الإنترنت بفضل التفاعل مع الآخر ووجود مجتمعات تؤثر في بعضها البعض في بيئة تفاعلية قد اثر بشكل كبير على تغيير الثقافة اكبر من البث الفضائي والتليفزيون الذي يتعتبر تأثرا سبلبيا بيد ان الإنترنت يعتبر تأثرا ايجابيا فبإمكانك استخدام المعلومات التي تجمعها من الإنترنت في التعرف على حقائق كثيرة فانت تشارك في صنع قرارك وسيكون من الصعب السيطرة على تفكيرك إذا كنت تعي ماذا تقرأ وماذا تفعل على الإنترنت.

يمكننا فعلا ان نقول بكل ثبات بأن هذا الإبتكار "الإنترنت" قد غير في ثقافة المجتمع حيث غير في ثقافة المجوعة لانه غير في ثقافة الفرض نظرا لتقريب المسافات فلم يعد من الصعب ان تنتمي إلى مجتمع او افكار معينة بسبب المسافات والتكلفة وما إلى ذلك فالأمر بوجود الإنترنت اصبح اسهل واسرع من ذي قبل.

فاصبح الآن تشكيل الفرق والجماعات والأفكار والمذاهب اسهل بكثير مما خلق ثقافات جديدة سواء على مستوى المجتع في اطار الاعمال او ثقافة الفرد كأنسان. واصبح الإنترنت ايضا مجالا جديدا للبحث عن فرص عمل بثقافة جديدة ومعطيات جديدة اثرت

ايضا في تفكير الفرد داخل المجتمع فعلى سبيل المثال تجد الآن عملة مالية للإنترنت وطرق حديثة في التعامل مع التجارة الإليكترونية والمتجر الإليكتروني والحكومة الإليكترونية وكل ما هي في ارض الواقع اصبح من الممكن ان يكون اليكتروني!

ومن اكثر الاشياء الملحوظة في الإنترنت هي سهولة تبني مذهبا او فكرة معينة والإنضمام إلى مجتمع يدعم هذه الفكرة بسهولة وعلى النقيض يسهل ايضا الإنفصال عن هذه المجموعة بسهولة مما جعل تغيير الهوية اسهل من ذي قبل لدى الفرد وهذا ادى إلى ظهور الكثير من الهويات المزيفة على الإنترنت والتي جعلت من الضروري التدقيق فميا تتعامل معه على الإنترنت حيث خلقت من الإنترنت ساحة لا يستهان بها في الإحتيال والتخفي والجريمة ايضا...مما ادى إلى حاجة ملحة في ظهور ثقافة الدفاع على الإنترنت والقانون على الإنترنت والحماية على الإنترنت...

واثر هذا في سلوك الفرد والمجتمع ايضا حيث ظهرت ايدولوجيات جديدة لم تكن موجودة من قبل او ان صح التعبير انتقلت ايدولوجيات بكاملها من ساحات الحياة الواقعية إلى ساحة الإنترنت مثل الجرائم الإليكترونية والإرهاب الإليكتروني والجهاد على الإنترنت وهذا بدورة ينقل ثقافات مختلفة قد تكون غير طافية على السطح كما اشرنا ولكن اصبح لها وجود ربما ظاهر في الإنترنت وقد تطور الامر إلى وجود حروب على الإنترنت في اوقات الصراع على ارض الواقع كساحة للحرب من اطراف اخرى تهتم بالنزاع على ارض الواقع واشهرها النزاع الفلسطيني الغسرائيلي والحرب الإليكترونية الدائة بينهما Cyber War وهذا يعكس مدى تاثير شقافة الإنترنت على المجتمعات والافراد حتى في احلك الظروف!

إلا اننا في مجمل القول يمكننا ان نقول ان الإنترنت قد اثر في حياتنا وفي ثقافاتنا وهو اداة لا يستهان بها سواء بالتأثير السلبي او الإيجابي وهو يعكس سلوك الفرد والجماعة والمجتمع فهو اداة يمكن توظيفها لتشويه الصورة وتحسينها على حد سواء.

ويبقى الفيصل في الامر من يستطيع ان يفرض ثقافته على الآخر!

من اهم المصادر: BERMAN Center for Internet & Society

جامعة هارفارد

http://cyber.law.harvard.edu

بقلم: اسك بي سي

ISSA™
Information Systems Security Association
The Global Voice of the Information Security Profession

منظمة امن نظم المعلومات
الآن في مصر...

Training Tomorrow's Security Professionals...

The largest organization for IS Security Professionals
More than 140 chapter in 35 countries
Now in Egypt!

امن المعلومات يبدأ بالتوعية والتدريب
دورات متخصصة ومعتمدة عالميا
شهادات معتمدة من اعرق المؤسسات العالمية

ASK PC

BRITISH INSTITUTE FOR LEARNING & DEVELOPMENT
ORGANISATIONAL MEMBER

BCS
REGISTERED COURSE PROVIDER

IEEE

Founding Sponsor & Course Provider

ISSA in Egypt:
38 Mustafa El Nahas Street,
Floor 5, Nasr City, Cairo

+20 2 22715443
+20 12 4473366

www.issa-eg.org