أمن وسـرية البيانات والمعلومات

م. معاذ مصطفى سـليمان

مركز الحاسـوب-الجامعة الاردنية

المدرب

- مواليد 1976- اربد
- خريج جامعة العلوم والتكنولوجيا الاردنية
  - بكالوريوس هندسة كهربائية (تخصص حاسوب) 1999
  - ماجستير هندسة الحاسوب 2007
- حاصل على شهادات عالمية (CITM,CDCP,MCSE,MCSA,CCNA)
- المشاركة في العديد من الدورات الفنية والورشات التدريبية داخل وخارج الأردن (بريطانيا، كوريا، لبنان، الامارات)
- إعطاء العديد من الدورات في مجال إدارة وهندسة نظم مايكروسوفت(System Administration & Engineer)
- أعمل حاليا مدير دائرة ضمان الجودة و الخدمات الفنية في مركز الحاسوب- الجامعة الاردنية

بعض مصلحات أمن المعلومات

1. **السرية أو الموثوقية (Confidentiality):** التأكد من أن المعلومات لا تكشف ولا يطلع عليها إلا أشخاص مصرحين بذلك .
2. **التكاملية وسلامة المحتوى Integrity:** التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به.
3. **استمرارية توفر المعلومات أو الخدمة Availability:** التأكد من استمرار عمل النظام المعلوماتي.
4. **عدم الإنكار:** توفر القدرة على إثبات أن تصرفاً ما قد تم من شخص ما في وقت معين.

أمن المعلومات

1. على مستوى الأنظمة و الخدمات الالكترونية
2. على مستوى الافراد

الحماية الفيزيائية للخوادم و التجهيزات الحاسوبية والبيانات

- أنظمة الدخول الى غرفة الخوادم (Data Center Access control)
- أنظمة مراقبة بيئة التشغيل (Environmental Monitoring System)
- أنظمة التبريد(Cooling Systems)
- أنظمة مكافحة الحرائق (Fire Fighting systems)
- اعدادات حماية الوحدات التخزينية (RAID)
- أنظمة تزويد كهرباء (UPS & Generators)

بعض وسائل الحماية الالكترونية للبيانات

- Firewall Appliances (NGF)
- IPS/IDS
- AntiSpam
- AntiVirus
- Web Filtering
- Secure transmission of Data (SSL, HTTPS…)

طرق وسبل حماية جهاز الحاسوب

- الحماية الفيزيائية (Physical Security)
- حماية الجهاز من التعرض للصدمات والاهتزاز اثناء التشغيل
- عدم السماح للأشخاص غير الموثوق بهم لاستخدام الجهاز(Shoulder surfing, key loggers)
- إخفاء أجهزة المحمول في صندوق السيارة
- أغلق حاسوبك في حال ابتعادك عنه، ويفضل فصل مقبس الكهرباء عند عدم الحاجة للجهاز

طرق حفظ المعلومات -الافراد

1. وضع كلمة سر على النظام (يفضل البصمات البيولوجية مثل بصمة الاصبع والبصمة الصوتية)(Screensaver pwd).
2. وضع برنامجٍ موثوقٍ لمقاومة الفيروسات الإلكترونية الضارة.
3. حماية الدخول إلى شبكة الإنترنت والتأكد من مصادر البريد الإلكتروني.
4. يضاف للنظام جدران نارية.
5. تكوين تقنيات التشفير المناسبة.

حماية البيانات من خلال نظام التشغيل وبرامج الحماية

- استخدام نظام تشغيل حديث وفحص التحديثات المتوفرة باستمرار
- العمل بصلاحيات مدير النّظام(Administrator): دعوة للاختراق
- انشاء المستخدمين وإعطاء الصلاحيات
- استخدم كلمات مرور صعبة للدخول الى سطح المكتب
- كن حذراً عندما يعطيك احدهم ذاكرة متنقلة (USB Flash stick)
- عدم التخزين على C:\
- النسخ الاحتياطي للملفات المهمة باستمرار
- تشفير Encryption البيانات المهمة

نصائح استخدام كلمات المرور

1. استخدم كلمة سر مكونة من 6 خانات على الاقل .
2. استخدم كلمة سر تحتوي على حروف وارقام ورموز خاصة مثل (&*$@#) .
3. لا تفصح لاحد عن كلمة السر الخاصة بك.
4. كلمة السر تحفظ في الذاكرة لا تكتبها ابدا ، او تتركها في مكان مكشوف.
5. قم بتغيير كلمة السر الخاصة بك بشكل دوري او كلما اقتضت .
6. قم بالتغطية اثناء ادخالك لكلمة السر.

نصائح استخدام كلمات المرور

- 7. لا تستخدم كلمة سر من السهل تخمينها مثل (اسم والدك، اسمك، رقم الهاتف، تاريخ الميلاد).
- 8. لا تستخدم حروف وارقام متكررة مثل (aaa،1234)
- 9. اعلم ان كلمة السر الضعيفة يمكن للمخترق الحصول عليها بسهولة.
- 10. معظم المواقع تقدم خدمة تذكير في حال نسيان كلمة المرور ، فكن حذرا من اختيارك للأسئلة التذكيرية لكلمة السر بحيث لا تكون قابلة للتخمين مثل (اذا اخترت اسم والدك كجواب لسؤال التذكير ، كن حذرا ممن يعرفون هذه المعلومة).
- 11. عند تغيير كلمة السر استخدم كلمة سر تختلف عن السابقة.

2014 **"Worst Passwords"**

- 1 123456 (Unchanged from 2013)
- 2 password (Unchanged)
- 3 12345 (Up 17)
- 4 12345678 (Down 1)
- 5 qwerty (Down 1)
- 6 1234567890 (Unchanged)
- 7 1234 (Up 9)
- 8 baseball (New)
- 9 dragon (New)
- 10 football (New)
- 11 1234567 (Down 4)
- 12 monkey (Up 5)
- 13 letmein (Up 1)

- 13 letmein (Up 1)

- 14 abc123 (Down 9)
- 15 111111 (Down 8)
- 16 mustang (New)
- 17 access (New)
- 18 shadow (Unchanged)
- 19 master (New)
- 20 michael (New)
- 21 superman (New)
- 22 696969 (New)
- 23 123123 (Down 12)
- 24 batman (New)
- 25 trustno1 (Down 1)

الربط على الشبكة (المحلية او الانترنت)

- مشاركة الملفات والاطلاع على ال (Open Sessions)
- أهمية السجلات واستخدامها (Logs)
- كلمات المرور Pass Words
- جدران الحماية Firewalls
- التحديث التلقائي Automatic Update
- التشفير Encryption

Malware

- Viruses
- Worms: not attached to files, affect network
- Trojans: misrepresents itself to appear useful, do not attempt to inject themselves into other files or otherwise propagate themselves
- Spyware: tracking and storing Internet users' movements on the Web and serving up pop-up ads to Internet users
- Adware

- Delete /Encrypt files
- Send emails
- Install backdoors(become part of Zombie network)
- Slower performance
- Denial of Service
- Targeted attacks
- Annoying popups and Ads

الاحتيال الالكتروني
سرقة الهوية / انتحال الشخصية Identity Theft

- هي نوع من الجرائم تهدف الى الحصول على البيانات والمعلومات الشخصية الخاصة بك ، وبالتالي يتمكن المجرم من انتحال شخصيتك واستغلال تلك البيانات والمعلومات في الخداع بهدف تحقيق مكاسب مالية غير مشروعة ، من الامثلة على البيانات الشخصية المعرضة للسرقة:

1. رقم الحساب
2. اسم المستخدم، كلمة السر، تاريخ الميلاد.
3. رقم بطاقة الائتمان

الاحتيال الالكتروني
التصيد عبر الانترنت (Phishing)

- التصيد او الاحتيال الالكتروني هو نوع من الخداع على شبكة الانترنت حيث يقوم المحتالون بإرسال الآلاف من رسائل البريد الالكتروني مغشوشة التي تظهر بأنها مصدر موثوق، مثل البنك الذي تتعامل معه وتطلب تقديم معلومات شخصية او تطلب إتباع رابط يوجهك الى مواقع مزيفه انشأت لأغراض الاحتيال

- الهدف: الحصول على بيانات المستخدم الشخصية مثل رقم بطاقة الائتمان ، كلمة السر ، من اجل استخدامها في أغراض احتيالية غير مشروعة.

افضل الممارسات لتجنب الوقوع في عمليات الاحتيال عبر الانترنت

1- لا تثق باي رسالة او اي شخص يطلب منك معلومات شخصية عبر الهاتف ، حتى لو وصلتك رسالة الكترونية من بريد الكتروني يطلب منك معلومات شخصية حتى وان كانت من شخص تعرفه.

2- قم بإتلاف كشف حسابك او البيانات الشخصية غير الضرورية بشكل امن.

3- راقب حساباتك البنكية واطلب كشف بالحركات المالية بشكل دوري.

4- تفقد فواتير مشترياتك للتأكد من عدم وجود مشتريات لم تقم بشرائها.

5- لا تحمل بيانات حساسة او كلمة السر في محفظتك او حقيبة اليد.

6- اشترك في خدمات الرسائل القصيرة SMS لمراقبة الحركات التي تتم على حسابك البنكي

افضل الممارسات لتجنب الوقوع في عمليات الاحتيال عبر الانترنت

7- تجنب الدخول الى الخدمات المصرفية الخاصة بك من الاماكن العامة مثل مقاهي الانترنت.

8- عند عملية الشراء عبر الانترنت حاول ان تستخدم بطاقة شراء خاصة تصدرها البنوك لهذه الغاية ، وعدم استخدام بطاقة الائتمان البنكية.

9- لا تحتفظ برقمك السري على جهاز الهاتف المحمول او جهاز الكمبيوتر المحمول بشكل واضح ومفهوم الدلالة.

10- لا تدخل معلومات شخصية او الرقم السري من خلال القنوات الالكترونية والانترنت الا اذا بدأ الموقع ب\\:HTTPS

11- قم بالضغط على خيار(Log out)عند الانتهاء من استخدام الخدمة وتأكد من انك قمت بالخروج من الخدمة عند عدم ملازمتك جهاز الحاسب.

تذكر : لن يطلب منك البنك إعادة تفعيل حسابك او إعادة إدخال بياناتك او رقم بطاقة الائتمان، او رقم حسابك المصرفي، كما لن يقوم بطلب اسم المستخدم (User Name)او رمز الدخول (Password)الخاصة بك على الإطلاق.

E-mail Safe Browsing Habits

- Don’t open e-mails from people you don’t know.
- Don’t open e-mail attachments from people you don’t know.
- Beware of e-mail attachments from people you do know, but seem out character for them, ask for verification.
- If opening e-mails from people you don’t know, which is a necessary at times, consider using a virtual machine to open e-mails.
- Don’t pass on “chain letters” or forwards, at least not messages that have no informative value.

Social Networking Safe Browsing Habits

- Be careful who you add as a friend to your social networking contacts.
- Keep a close eye on what applications you add, as they may include spyware and grayware, i.e., games
- Watch out for strange messages from your friends/family which are full of spelling and grammar error, which contain links to external page

Phishing IQ Test

- http://www.sonicwall.com/phishing/

تأمين هاتفك الذكي

- ضع كلمة مرور أو رقم تعريف (PIN)
- حاول تثبيت برنامج لمكافحة الفيروسات والبرمجيات الضارة الاخرى من مرزوّد خدمة موثوق
- حدّث نظام التشغيل الذي يستخدمه هاتفك بشكل دوري
- اذا كنت لا تستخدم خاصية بلوتوث أو خاصية تحديد المكان فقم بتعطيلهما. فعّل احداهما أو كلاهما عند الحاجة فقط
- استخدم خاصية المسح عن بعد (remote wipe) اذا كان هاتفك أو مزوّد الخدمة يدعم هذه الخاصية
- شفّر بياناتك. بعض الهواتف تسمح لك بتشفير البيانات المخزّنة على الهاتف نفسه أو على الذاكرة المتنقلة
- قم بعمل نسخة احتياطية من بياناتك بشكل دوري.
- لا تقم بتحميل برامج قبل ان تعرف ما هي الصلاحيات التي تتطلبها هذه البرامج
- تأكد من البرامج التي تقوم بتحميلها. (الشركة المصنعة، عدد المستخدمين، نسخة الإصدار...)

تأمين هاتفك الذكي

بعض علامات على أن هاتفك مصاب ببرمجيات ضارة

- هناك ارتفاع مفاجئ في فاتورة هاتفك بدون سبب واضح
- هناك رسائل الكترونية او نصية في مجلد المرسل لم تقم أنت بإرسالها
- واجهة هاتفك تغيرت ولم تقم أنت بهذا التغيير.

Year 2015 in figures

According to Kaspersky Lab, in 2015

- **The proportion of spam in email flows was 55.28%, which is 11.48 percentage points lower than in 2014.**
- **79% of spam emails were no more than 2 KB in size.**
- **15.2% of spam was sent from the US.**
- **146,692,256 instances that triggered the 'Antiphishing' system were recorded.**
- **Russia suffered the highest number of phishing attacks, with 17.8% of the global total.**
- **Japan (21.68 %) took the lead in the ranking of unique users attacked by phishers.**
- **34.33% of phishing attacks targeted online financial organizations (banks, payment systems and online stores).**

You Tube Videos

- email phishing
- https://www.youtube.com/watch?v=9TRR6lHviQc#action=share
- https://youtu.be/E-L8Rrv6A8w
- Strong Passwords
- https://youtu.be/aEmF3lylvr4
- https://www.youtube.com/watch?v=VYzguTdOmmU
- How To Make An Auto Hacking USB Drive
- https://www.youtube.com/watch?v=lFlgddjOPpw
- Password Cracking 101
- https://www.youtube.com/watch?v=97CdJFyAv1s
- Safe on your mobile
- https://www.youtube.com/watch?v=gOTRBGsj0B4
- https://securelist.com/analysis/kaspersky-security-bulletin/73591/kaspersky-security-bulletin-spam-and-phishing-in-2015/