ورقة علمية بعنوان

الأمان في الهاتف المحمول

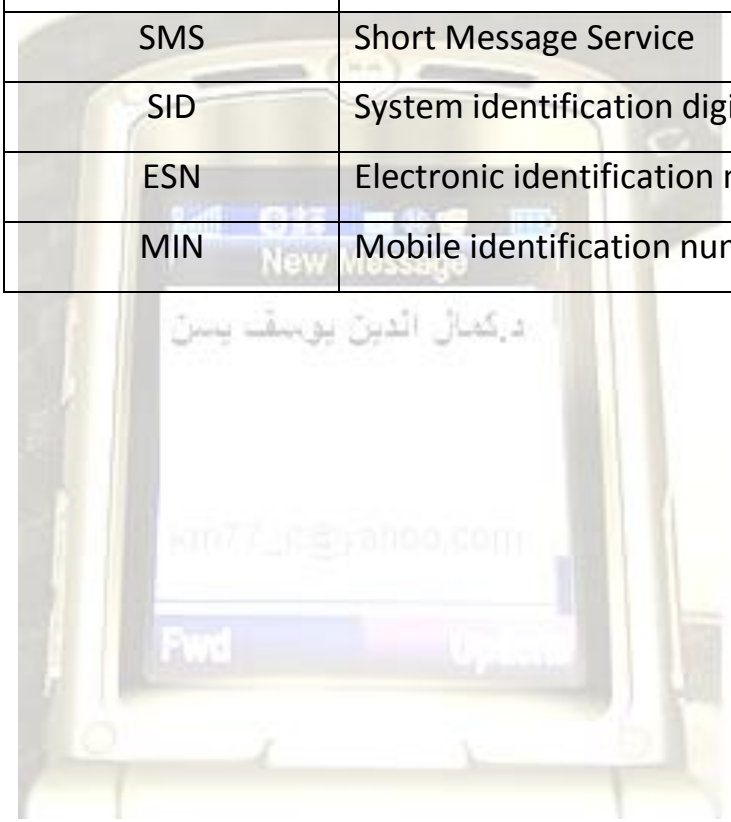
إعداد الدكتور

كمال الدين يوسف يسن

2011م

مَسرَدُ المُصطلحاتِ التِّقنيّةِ

المصطلحات	الترجمات الانجليزية	الترجمة العربية
MZ	Mega herz	ميقا هيرز
mp3	**MPEG-2.5 Audio Layer III**	ملفات الصوت الرقمية
wav	**Waveform Audio File Format**	نظام ملفات الصوت
SMS	Short Message Service	خدمة الرسائل القصيرة
SID	System identification digit	شيفرة نظام التعريف
ESN	Electronic identification number	الرقم التسلسلي الالكتروني
MIN	Mobile identification number	رقم تعريف الجوال



hacker	"الهكرة" هم شُطّارٌ لديهم دراية عميقة بالحوسبة و الشبكات و البرمجة أو بإحدى مجالاتها، و مهارة في استخدام تقنيات المعلوماتية و قدرة على إيجاد حلول مبتكرة للمشكلات، و ليسوا بالضرورة مخربين و لا خارجين على القانون، إلا أنه في هذا السياق يقصد بهم كل من يسعى إلى النفاذ إلى حواسيب أو نظم ليست لديه صلاحية النفاذ إليها أو الاطلاع على معلومات لم يُصرَّح له بالاطلاع عليها، أيا كان غرضهم من وراء ذلك.
malware	برمجية كتبت لتخدم غرض المتحكم فيها بغض النظر عن مصلحة صاحب النظام الذي تصيبه أو تعمل فيه، و تشمل الفيروسات و الديدان و أحصنة طروادة و البرمجيات التجسسية و غيرها.
spyware	فئة من البرمجيات الخبيثة صُممت بحيث تنقل إلى من يتحكم فيها بيانات من نظام يخص غيره بلا علم مالك النظام المصاب أو رغبته. قد يكون الدافع إلى ذلك هو الفضول، أو أغراضا أمنية، أو أغراضا تسويقية تجارية؛ و ذلك عادة باستخدام وظائف الاتصالات المتاحة للنظام المصاب. من أمثلة البيانات التي تصمم البرمجيات للحصول عليها: المراسلات، و كلمات السر، و البيانات المالية، و أنماط تصفح الإنترنت و استخدام

مخترق

برمجية خبيثة

برمجية تجسسية

البرمجيات الأخرى.

key logger	أداة تُزرع في حاسوب بغرض تسجيل ضربات أزرار لوحة المفاتيح أثناء استخدام الحاسوب على أمل التقاط بيانات سرية يصعب الحصول عليها بوسائل أخرى - مثل كلمات السر - لحظةَ إدخالها، ثم إرسال ذلك السِّجِل إلى من يتحكم في أداة التجسس هذه، إما عبر الشبكة أو بأن يسترجع بنفسه ملف السجلَّ إن كان له نفاذ مادي إلى الحاسوب المستهدف.
FOSS (*F*ree*O*pensource*S*oftware)	برمجية مجانية و مفتوحة المصدر؛ منشورة برخص حرة تسمح لأي شخص باستخدامها و نسخها و توزيعها مجانيا دون مقابل و دون أن يكون بذلك معتديا على حق مؤلفها أو مخالفا قوانين حماية الملكية الفكرية. كما تنشر معها شفرتها المصدرية، بحيث يمكن لمن لديه الدراية التقنية تعديلها لتناسب استخداماته الخاصة، أو أن يحسنها أو يغير من الوظائف التي تؤديها أو يعالج العلات التي قد توجد فيها، أو أن يبني عليها برمجيات أخرى، و كل ذلك دون الرجوع إلى المؤلفين الأصليين، و بلا شرط سوى أن ينشر نتيجة عمله بذات الرخصة ليعطي غيره ذات الحقوق التي كان قد حصل عليها (غالبا، و حسب متطلبات كل رخصة.)
freeware	برمجية يسمح منتجوها باستخدامها مجانا، لكنهم

مُسَجِّل لوحة المفاتيح

برمجية حرة

برمجية مجانية

غالبا لا يتيحون شفرتها المصدرية للآخرين كما أنهم يحتفظون بكامل حقوق الملكية الفكرية لها، و قد يسمحون للمستخدمين بنسخها و إعادة توزيعها كما هي دون تعديل فيها.

firewall	برمجية قد تعمل في واحدة أو أكثر من طبقات النموذج الشبكي (OSI) تقوم بدور حارس الحدود لنظام الحاسوب أو الشبكة لتراقب و تتحكم في مرور تدفقات البيانات الواردة و الصادرة منه و إليه وفق قواعد يحددها المستخدمُ مديرُ النظام. قد تشمل القواعد طبيعة الاتصال من حيث كونه واردا أو صادرا، أو الطرف الآخر من الاتصال، أو فحوى الاتصال، أو التطبيق المتصل، أو الوقت، أو هوية المستخدم، أو توافيق من هذه المعايير و غيرها.
port	مدخل منطقي إلى النظام الحاسوبي يُستخدم للاتصال بين التطبيقات الشبكية، بعض أرقام المنافذ قياسي و يرتبط بخدمات محددة، مثل 80 لأجل الوب و 23 لأجل تِلنِت.
route	المسار المنطقي الذي تتخذه تدفقات البيانات عبر الشبكة من عقدة إلى عقدة.
modem	نبيطة أو برمجية لترميز البيانات و عكس ترميزها وفقا لبروتوكولات اتصالات معروفة، تستخدم للاتصال بين الحواسيب. الكلمة الإنجليزية نحتُ

جِدار النار

منفذ

مسار

مُودِم

من الكلمتين modulator و.demodulator

router	مُسيِّر	نبيطة أو برمجية في شبكات تسيير الرُّزَم (packet switching network)يُمرر الرزم (وحدات الاتصال) بناء على عناوين وجهاتها، و يستخدم لوصل الشبكات المحلية و الحواسيب بإنترنت. يوجد مُسيِّر في أجهزة الوصلات السريعة بإنترنت (مثل DSL و ما شابهها.(
device	نبيطة	جهاز عتاد يشكل جزءا من منظومة حاسوبية أو شبكية و يؤدي فيها وظيفة محددة، مثل تخزين البيانات أو تمريرها عبر الشبكة أو معالجتها بأي شكل. يمكن أن تكون النبيطة افتراضية، أي مُحاكاةً بالبرمجيات بدلا من أن تكون عتادا ماديا، إلا أن المكونات الأخرى في النظام تتواصل معها بذات البروتوكولات كما لو كانت عتادا ماديا. من أمثلة نبائط التخزين مشغلات الأقراص و شذرات ذواكر يوإسبي، و من النبائط الشبكية المودمات، و بطاقات شبكة، و من النبائط البصرية الماسحات و كاميرات الوب.
sourcecode	كود المصدر (أو شفرة المصدر(	هي مجموع التعليمات التي تؤلف برمجية ما و التي يكتبها المُبرمِجُ بناء على منطق تصميمي معين ليأمر الحاسوب بتنفيذ وظائف الحوسبة الأساسية، من إدخال و معالجة و إخراج و تخزين البيانات، بتسلسل معين و وفق شروط معينة بما يحقق الغرض من البرمجية، و ذلك باستخدام

	واحدة أو أكثر من لغات البرمجة، و أنماط البرمجة.	
LiveCD	قرصٌ مدمجٌ عليه نظام تشغيل يمكن تشغيله بإقلاع الحاسوب من القرص مباشرة دون الحاجة إلى تنصيبه أو تغيير تهيئة و إعدادات و تضبيطات الحاسوب، و ذلك بشكل مؤقت، ثم الرجوع إلى الحالة الأصلية بإعادة تشغيل الحاسوب.	قرص حيّ
physical threats	كل ما يتهدد البيانات نتيجة أفعال من لديهم نفاذ مادي إلي الحواسيب و وسائط التخزين، و كذلك كل الأحداث المادية التي يمكن أن تخرب العتاد مثل الحوادث و الكوارث الطبيعية و التخريب المتعمد.	تهديد مادي
wireless access point	نبيطة شبكية تتيح اتصال الحواسيب و الأجهزة الشبكية الأخرى في شبكة حاسوبية محلية لاسلكية، و قد تكون متصلة بأجهزة تستخدم كمخارج اتصال لاسلكي بشبكات خارجية أو بالإنترنت.	نقطة اتصال لاسلكي
*M*edia *A*ccess*C*ontrol address	مُعرِّف شِبه فريد يميز كل نبيطة شبكية يستخدم لتعريف النبيطة في سياقات الاتصال المختلفة. بطاقات الشبكات و المسيرات و غيرها من نبائط شبكية لكل منها عنوان شبه فريد يوضع فيه عند تصنيعه و لا يمكن تغييره إلا بصعوبة.	عنوان التحكم في النفاذ للوسيط
server	مكوِّن يعمل في منظومة ليؤدي وظيفة معينة بالاستجابة لطلبات مكونات أخرى في النظام،	خادوم

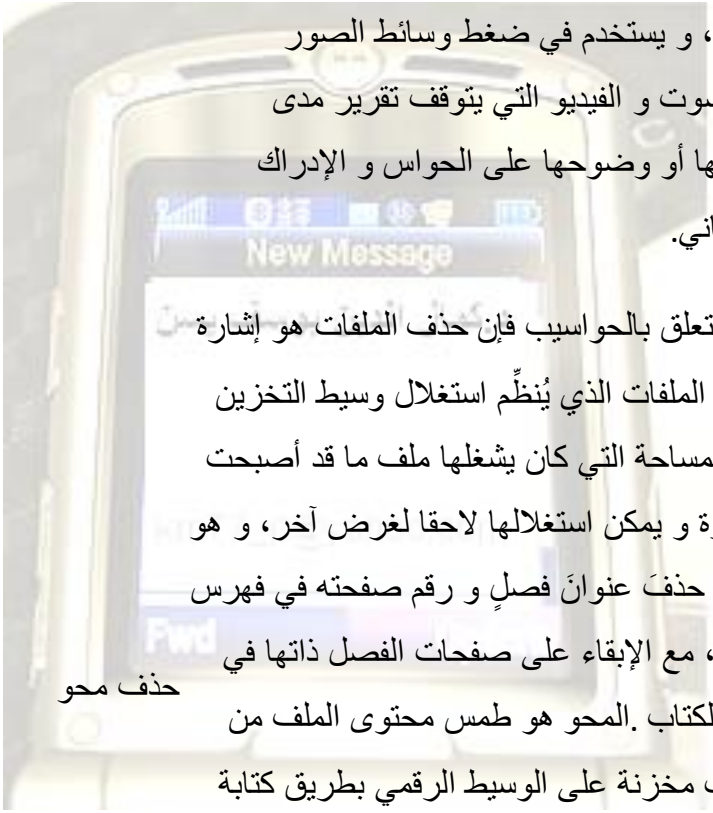
	و يتواصل معها ببروتوكول معين. قد يكون الخادوم برمجية أو عتادا.	
BIOS (*B*asic*I*nput/*O*utput*S*ystem)	الطبقة الأدنى من البرمجيات في نظام الحاسوب الشخصي الذي تنبني عليها المستويات الأعلى من الوظائف، و يشمل تحكمات تحدد تفعيل أو تعطيل جوانب من الوظائف الأساسية و سلوك العتاد	نظام الإدخالالإخراج الأساسي
*U*ninterruptable*P*ower *S*upply	نبيطة تتكون من مراكم للطاقة الكهربية و متحسسات لانقطاع التيار، و هي تُوصَل ما بين الأجهزة المراد حمايتها من تذبذبات التيار الكهربي و المأخذ الرئيسي فتنشحن مراكمها تلقائيا طالما استمر التيار، و فور تحسسها انقطاع التيار من المأخذ تتولى لحظيا إمداد الطاقة إلى الجهاز المتَّصل بها فلا يتعطل عمله لمدة معينة تعتمد على كم الطاقة المخزنة بالمركم.	مصدر تيار غير منقطع
volume	جزء منطقي في وسيط تخزين يستوعب داخله أجزاء منطقية أخرى للبيانات مثل الأدلة (directories)و الملفات .(files) عادة ما ينشأ المجلد في قسم (partition) على وسيط التخزين، و قد يشغل أكثر من قسم في بعض النظم. (لاحظ أن وثائق ويندوز أصبحت تستخدم "مجلد" كمقابل "directory" ("دليل") خلافا لما استقر طويلا في نظم التشغيل الأخرى مما يسبب لبسا لقراء الأدلة التقنية.)	مجلَّد

resolution	مَيْز	الكثافة النقطية في الصورة الرقمية، سواء المحفوظة في ملف رقمي أو التي تستطيع طابعة إنتاجها، أو ماسحة ضوئية رقمنتها، أو كاميرا تسجيلها. و هي إحدى محددات جودة الصورة إذ تتناسب معها طرديا، و معها الذاكرة اللازمة لتخزينها. محدد آخر لجودة الصور الرقمية هو العمق اللوني.
encryption	تعمية	تطبيق حُسبانات رياضياتية على البيانات الرقمية لتحويلها من صيغتها الصريحة المقروءة إلى صيغة لا يمكن قراءتها إلا بتظهيرها، أي عكس التعمية، لردِّها إلى صيغتها الأصلية و هو ما يتطلب معلومة سرية، مثل كلمة السر أو المفتاح. توجد خوارزميات عديدة لإجراء حُسبانات التعمية لكنها عموما تنقسم إلى نوعين أساسسين: تعمية تناظرية، و تعمية بالمفتاح العلني (غير تناظرية.)
digital certificate	شهادة رقمية	وثيقة رقمية غير قابلة للتزييف تُطبِّق تقنية التوقيع الرقمي تفيد في التصديق على الوثائق الرقمية الأخرى و الأكواد البرمجية و توفير وسيلة للتحقق من أصالتها و مطابقتها للأصل الصادر عن الجهة الموقِّعة، و كذلك في استيثاق المراسلات بين الأفراد و النظم الحاسوبية.
digital signature	توقيع رقميّ	تقنية مبنية على التعمية بالمفتاح العلني تستخدم للتصديق على الوثائق الرقمية و المراسلات و للاستيثاقمن هويات المتراسلين لدرء التزييف

	و انتحال الهوية؛ و يمكن استخدامها لإلزام المُوقِّع بمضمون ما وقَّعه.	
authentication	صيرورة يمكن بها التيقن من صدق هوية الشخص أو الجهة أو النظام الحاسوبي حسبما يدّيعه، لدرء انتحال الهوية، و ذلك إما بإبراز معلومات سرية يتفق عليها الطرفان مسبقا، أو باستخدام الشهادات الرقمية.	استيثاق
steganography	أساليب لتمويه البيانات و إخفاءها في بيانات أخرى فلا يمكن للمهاجم معرفة وجودها من عدمه، و توجد لذلك عدة أساليب و تقنيات.	(إخفاء البيانات)
plausible deniability	عدم القدرة على إثبات ادعاءٍ ما (عادة اتهاما) على من يُنكره، مع عدم القدرة على إثبات نفيه عمليا؛ و يمكن أن ينطبق في الحالات التي تنطبق فيها القاعدة القانونية الناصة على أن الشك في صالح المتهمو أن البَيِّنة على من ادّعى.	حجية الإنكار
proxy server	خادوم على الإنترنت يقوم بدور وسيط ما بين خادوم و عميل. تستعمل الخواديم الوسيطة لأغراض عديدة، منها تخفيف العبء عن خواديم المحتوى و التطبيقات، و كذلك في تجاوز الرقابة على محتوى الإنترنت.	خادوم وسيط
data compression	هو تطبيق حُسبانات رياضياتية على البيانات لتحويلها إلى شكل يشغل حيزا أقل عند تخزينها على الوسائط الرقمية أو عند نقلها، ثم يمكن	ضغط البيانات

إعادتها إلى صيغتها الأصلية بخوارزميات أخرى.

يوجد نوعان رئيسيان من الضغط، أحدهما الضغط غير الفقود (lossless) الذي يقلل حجم البيانات دون فقد أي قدر منها و بحيث تطابق البيانات بعد إزالة الضغط عنها البيانات الأصلية قبل الضغط؛ و الآخر الضغط الفقود (lossy) الذي يُفقَد أثناء إجرائه قدر من البيانات، بهدف تقليل الحجم بدرجة كبيرة، و يستخدم في ضغط وسائط الصور و الصوت و الفيديو التي يتوقف تقرير مدى جودتها أو وضوحها على الحواس و الإدراك الإنساني.



deletion vs. wiping

حذف محو

فيما يتعلق بالحواسيب فإن حذف الملفات هو إشارة لنظام الملفات الذي يُنظِّم استغلال وسيط التخزين بأن المساحة التي كان يشغلها ملف ما قد أصبحت شاغرة و يمكن استغلالها لاحقا لغرض آخر، و هو يماثل حذفَ عنوانَ فصلٍ و رقم صفحته في فهرس كتاب، مع الإبقاء على صفحات الفصل ذاتها في متن الكتاب .المحو هو طمس محتوى الملف من بيانات مخزنة على الوسيط الرقمي بطريق كتابة بيانات أخرى فوقها، و هو الأسلوب الآمن لتدمير البيانات و ضمان - أو تقليل احتمال - أن يتمكن شخص من استرجاعها باستخدام التقنيات المتاحة المعروفة.

swap file

ملف مبادلة

"المبادلة (swapping) "أسلوب تستخدمه نظم التشغيل لزيادة الذاكرة المتاحة لتشغيل التطبيقات

	باستخدام جزء من ذاكرة التخزين الثانوية المتمثلة في السواقات الصلبة للحفظ المؤقت لبعض محتوى الذاكرة الرئيسية المتمثلة في الرام (RAM) التي تعمل فيها التطبيقات، و التي عادة ما تكون أقل في السعة إلا أنها أسرع كثيرا، و بهذا يمكن للتطبيقات أن تستخدم قدرا من الذاكرة يفوق ما هو موجود فعلا في النظام.
cookies	)حرفيا: الكعكات) وسيلة تستخدمها المواقع على الوب لتخزين بيانات في المتصفح بهدف تسهيل استخدام تلك المواقع و إبداء استجابات ذكية لاختيارات و أفعال المستخدمين، و ذلك بحفظ تفضيلاتهم و أحيانا بيانات تخص حساباتهم. كوكيز
plug-in / extension / add-on	وحدة برمجية تضاف إلى برمجية لإضافة وظائف إليها أو تغيير سلوكها. الملحقات لا تعمل إلا في إطار البرمجية العائلة لها. مُلحقة
installation	صيرورة تجهيز البرمجية لاستخدامها في نظام حاسوبي. قد تكون صيرورة التنصيب بسيطة مما يُمكن إحراءه يدويا، من قبيل نسخ الملفات التنفيذية، أو استخراجها من حزمة التوزيع و فك ضغطها إلى موضع حفظها في النظام الذي تُنصَّب فيه، و قد تكون صيرورة معقدة تشمل عمليات نسخ عديدة في مواضع خاصة في النظام و إجراء إعدادت في مكوناته المختلفة، أو حتى ترجمة كود البرمجية من مصدره. لتسهيل عملية التنصيب توزع حزم تنصيب

البرمجيات متضمنة أداة تنصيب - مُنصِّبا - تنفذ المطلوب تلقائيا و قد تتفاعل مع المستخدم لمعرفة تفضيلاته. تتداخل مفاهيم "الإعداد (setup) "و "الضبط (configuration) "مع التنصيب عادة.

فتح حساب (أو "الاشتراك" أو "التسجيل") في خدمة ما على الإنترنت عبر موقع على الوِب أو تطبيق آخر يديره مقدّم الخدمة. عادة ما تتضمّن صيرورة فتح الحساب الإفصاحَ عن قدر ما من البيانات الشخصية، قد لا تزيد عن عنوان بريد إلكتروني، و قد تشمل تفصيلات أخرى عديد، كما تتضمن الموافقة على اتفاقية استخدامٍ تنشىء علاقة تعاقدية بين المستخدم صاحب الحساب و مقدّم الخدمة و تُنَظِّمها و تضع لها اشتراطات و حدودا و تبيّن حقوق و واجبات كل طرف فيها. على نحو ما يُنشئ الاشتراكُ في خدمةٍ هويةً رقميةً للمستخدِم تمثله في تلك الخدمة و في مجتمع المستخدمين الآخرين فيها. قد تشترط بعض الخدمات الإفصاح عن الاسم الحقيقي (القانوني) للمشترك أو لا و قد تشترط إظهاره للآخرين أو لا.

registration فتح حساب

دخول المستخدم إلى حسابه في خدمة عبر موقع إنترنت أو تطبيق حاسوبي آخر باستخدام بيانات تعرّفه و تبين لمدير الخدمة أحقيته في استخدام الحساب، بطريق اسم مستخدم مميز أو عنوان بريد إلكتروني و كلمة سر أو وسيلة استيثاق أخرى. بعد الولوج إلى الحساب قد تتبدى للمستخدم وظائف و

ولوج

معلومات و تحكمات في حسابه قد لا تكون ظاهرة للمستخدمين الآخرين غير الوالجين أو الوالجين بحسابات مختلفة. بولوج مستخدم إلى خدمته تنشأ جلية استخدام تنتهي بخروجه من الحساب.

المقدمة

الهاتف المحمول أو النقال أو الخلوي أو الجوال ويُقال في بعض اللهجات الموبايل أو البورتابل هو أحد أشكال أدوات الاتصال والذي يعتمد على الاتصال اللاسلكي عن طريق شبكةمن أبراج البث الموزعة ضمن مساحة معينة. مع تطور أجهزة الهاتف النقال أصبحت الأجهزة أكثر من مجرد وسيلة اتصال صوتي بحيث أصبحت تستخدم كأجهزة الحاسوب الكفيّ للمواعيد واستقبال البريد الصوتي وتصفح الشابكة والأجهزة الجديدة يمكنها التصوير بنفس نقاء ووضوح الكاميرات الرقمية،كما قد أصبحت الهواتف النقالة أحد وسائل الإعلان كذلك وبسبب التنافس الشديد بين مشغلي أجهزة الهاتف النقال أصبحت تكلفة المكالمات وتبادل المعطيات في متناول جميع فئات المجتمع. لذا فإن عدد مستخدمي هذه الأجهزة في العالم والعالم العربي يتزايد بشكل يومي ليحل محل أجهزة الاتصال الثابتة.

يعود تاريخ الهاتف المحمول إلى عام 1947 عندما بدأت شركة لوست تكنولوجيز التجارب في معملها ب«نيو جرزي» ولكنها لم تكن صاحبة أول خلوي محمول بل كان صاحب هذا الإنجاز هو الأمريكي مارتن كوبر الباحث في شركة موتورولا للاتصالات في شيكاغو حيث أجري أول مكالمة به في 3 أبريل عام1973.

المبدأ الرئيس في الهاتف النقال يعتمد على دائرة استقبال وإرسال عن طريق إشارات ذبذبة عبر محطات إرسال أرضية ومنها فضائية تماما مثل إشارات المذياع لكن الخلوي وشبكاته الأرضية يختلف عنهم وإشارات ذبذبية مثل رسم القلب تصاعدي وتنازلي وهي قوية جدا تصل إلى 20 MZإرسالا واستقبالا في الثانية الواحدة أما عن طريقة الاتصال فتكون عن طريق دائرة متكاملة تكمن في المحمول الشخصي والسويتش الرئيسي الخاص بالشركة والخط) بطاقة السيم (وهي بطاقة صغيرة بها وحدة تخزين

صغيرة جدا ودقيقة ووحدة معالجة تخزن بها بيانات المستخدم الذي يستخدمه للاتصال بالآخرين أما عن خواص المحمول فيتكون من دائرة استقبال وإرسال ووحدة معالجة مركزية وفرعية ورامة وفلاش لتخزين المعلومات ويمكن كتابة الرسائل القصيرة والاستمتاع بخواص المحمول وهي:

الاتصال بالآخرين ورؤيتهم عن طريق الجيل الجديد من الأجهزة dct4 المزودة بقُمرات دقيقة

يمكن إرسال الرسائل القصيرة لأي مكان في العالم

التسلية بالألعاب وكذا ألعاب الجافا الحديثة

الاستماع إلى ملفات صوتية بامتدادت مختلفة (مثل mp3. wav. ogg) والاستماع إلى المذياع ومسجل الصوتيات وغيرها من الألعاب المشتركة بين الأجهزة وعبر خطوط الشابكة.

وتجدر الإشارة بأن الهاتف النقال قد صدرت عنه عدة دراسات تؤكد أن التعرض بشكل كبير لذبذبات البث أو وضع الهاتف نفسه بجانب قلب الإنسان مثلا قد يضر بصحتة وأحيانا يؤدى إلى حدوث أعطال بأجهزة تنظيم ضربات القلب.

تحديد المكان والحركة

يتم تحديد حركة الهاتف الجوال عند تنقله من مكان لآخر، وتقوم الخلايا بنقل المعلومات إلى الكمبيوتر المركزي الخاص بالشركة المقدمة لخدمة الاتصال، الذي يقوم بتسجيل وأرشفة هذه المعلومات أولا بأول، وبذلك تكون تنقلات هذا الجهاز وحركته معروفة ومحفوظة وبدقة لحظة بلحظة في أرشيف على ذاكرة الجهاز المركزي، ويمكن الرجوع إليها في أي وقت، يشمل ذلك أيضا تحديد موقع طرفي الاتصال.

كما وتستطيع أجهزة المخابرات الحصول على جميع المكالمات سواء السلكية أو اللاسلكية في أي وقت من السنة، من خلال الكمبيوتر المركزي، وتستطيع أيضا معرفة جميع الأرقام التي اتصلت بها واتصلت بك بزمنها الحقيقي، كذلك معرفة مكانك على الأرض، عن طريق الذبذبات التي يرسلها جوالك النقال من وإلى الخلايا المجاورة.

الرسائل القصيرة

تعتبرالرسائل القصيرة(SMS) نمط من أنماط الاتصالات التي ترسل نصاً بين الهواتف النقالة، أو من جهازكمبيوتر إلى هاتف نقال، فعندما يتم إرسال رسالة فإن جهاز الكمبيوتر المركزي يحتوي على مرشح للكلمات، قادر على تمييز الكلمات وفرزها وتصنيفها، وذلك أثناء إجراء المكالمة بناء على قائمة من الكلمات الموضوعة مسبقا على الكمبيوتر، وتضم هذه الكلمات ما تختاره أجهزة المخابرات مثل سلاح، عبوة، رصاصة، رمان،غزة،...إلخ (والمكالمات التي يتحدث أصحابها بهذه الكلمات، يتم فورا التنبه لها والاستماع لمضمونها، أيضا يستطيع الكمبيوتر أن يميز أي رسالة غامضة، وتحويلها إلى المراقبة.

كما تمكن الرسائل القصيرة المهاجم بتزيف الرسالة النصية لكي تبدو آتية من الشركة المقدمة للخدمة لإقناع الضحية بتنزيل البرنامج الضار، أو زيارة الموقع الذي تستضيفه. وفي أسلوب آخر استخدمت الرسالة النصية لإطلاق متصفح للشبكة على الجوال وتوجيهه إلى موقع يمكن أن يتضمن البرنامج الضار. وعندما يستخدم الأسلوب الهجومي هذا لاصطياد المعلومات الشخصية، فإنه يطلق عليه في هذه الحالة تعبير «سميشينغ.SMiShing »

الرسائل الإقتحامية(Mobile spam)

تشمل الرسائل الإقتحامية للجوال الرسائل النصية غير المرغوب فيها والتى ترسل إلى هاتفك الجوال دون طلب مسبق. وترسل معظم الرسائل الإقتحامية بواسطة شركات التسويق والإعلانات إلى آلاف المشتركين

بخدمة الهاتف الجوال كدفعة واحدة وفى وقت معين فى محاولة منهم للترويج لمنتجاتهم وخدماتهم. وفي معظم الحالات، ترسل هذه الرسائل بدون علم الشركة المسئولة عن تقديم خدمات الاتصالات وبدون أن يكون لها خيار لإيقاف استلام تلك الرسائل، وفيم يلي نماذج لبعض الرسائل الإقتحامية:

- "لقد فزت بمبلغ 500 الف ريال قطرى، اتصل بنا على هاتف رقم (xxxx) لتحصل على جائزتك".
- "تنزيلات وخصومات غداً بمحلات".(xxxx)
- "شخص ما يريد مقابلتك والتعرف عليك. اتصل بهذا الرقم ليمكنك " الدردشة" معه ومعرفة أشخاص جدد".

المكالمات "الخداعية(Mobile scam)

هى مكالمات سريعة تهدف الى خداع صاحب الهاتف الجوال للحصول على مكسب مادي والاسلوب الشائع في هذه المكالمات هو اسلوب الـ"missed call" ، فقد يتلقي المشترك مكالمة سريعة على هاتفه الجوال من جهة ما ويقفل الخط بسرعة بحيث لا يستطيع الرد عليها في حينها، وتسجل "كمكالمة لم يتم الرد عليها" من رقم غير معروف، وبمجرد معاودة الاتصال بذلك الرقم يجد المشترك نفسه قد اشترك دون قصد أو رغبة منه في خدمة معينة دون أن يكون له الخيار لوقف تلك الخدمة. وما يزيد الامور سوءاً هو أن يفاجأ المشترك بان عليه دفع فاتورة باهظة الثمن لخدمة لم يطلبها.

لذا يجب تجنب المكالمات الهاتفية غير المرغوب فيها التي تطلب سداد رسوم مسبقة من خلال رسائل نصية تعد المشترك بربح مبالغ مالية أو كسب أو كسب جائزة عينية شريطة دفع مبلغ محدد قبل الاستلام.

ففى الآونة الاخيرة، تلقى بعض مشتركي الهاتف الجوال فى الدوحة مكالمات هاتفية غير مرغوبة تبلغهم بأنه تم اختيارهم بطريقة عشوائية عن طريق شركة "فودافون" لكسب مبلغ من المال قدره 160,000 دولار

أمريكي. هذا ويطلب المتصل من المشترك إيداع مبلغ وقدره 6,000 ريال قطرى فى حساب بنكي معين للحصول على الجائزة المزعومة.

لذا يجب توخي الحذر لتفادي تلك العروض الخادعة هذه الخدع. ويود المجلس الأعلى للاتصلات وتكنولوجيا المعلومات أن يؤكد أن تلك العروض ليست مقدمة من شركة فودفون، وإنما ضرباً من الخداع تقوم به مجموعة من المحتالين عن طريق استخدام اسم شركة "فودافون" لخداع المشتركين وابتزاز أموالهم.

وفيمايلي نماذج للرسائل غير الإقتحامية:-

- الرسائل النصية التى تخص خدمة معينة بنكك الخاص أو جهة حكومية.
- رسائل نصية من شركة "كيوتل" بخصوص فاتورة الهاتف.

ماذا تفعل في حالة استلام رسائل اقتحامية أو مكالمات غير مرغوبة على جوالك؟

تفادى الرد على الرسائل من مصادر مجهولة أو من جهات لم تطلب منها خدمة معينة.

- لا تعاود الاتصال بالأرقام التى يسجلها جوالك من جهات مجولة. في حالة الرد قد تحسب المكالمة بتكلفة ساعة الذروة.
- اتصل بالشركة المذكورة في الرسالة مباشرة لتتحقق اذا ما كانت العروض المعلنة باسم الشركة حقيقية أم لا.

تجنب استلام الرسائل الاقتحامية والمكالمات غير المرغوبة

لا تفصح عن رقم هاتفك الجوال الخاص لمحلات التجارية أو المطاعم أو المواقع الالكترونية.

- لا تفصح عن رقم هاتفك الجوال عند تعبئة استبيانات أو المشاركة في استطلاعات الرأى.
- اطرح ما تود من أسئلة إذا ارتبت في شركة تطلب منك رقم هاتفك الجوال عند شراء خدماتها أو منتجاتها.

- اقرأ الرسائل الاقتحامية الواردة الى جوالك بعناية لمعرفة اذا ما كان هناك خيار لوقف استلام تلك الرسائل.

تقنية البلوتوث

البلوتوث هي تقنية لاسلكية تمكن من التواصل بين الأجهزة في مدى محدود، وهي تقنية منتشرة في أغلب الأجهزة الخلوية والكمبيوترات المحمولة لأنها تقدم سهولة التواصل بدون أسلاك، ويمكن استخدام تقنية البلوتوث لربط أنواع مختلفة من الأجهزة ببعضها مثل:

1. ربط هاتف جوال بسماعة الأذن.
2. ربط هاتف جوال بحاسوب محمول.
3. ربط جهاز حاسوب محمول بحاسوب عادي.
4. ربط لوحة المفاتيح بالحاسوب.
5. ربط الفأرة بالحاسوب.
6. ربط جوال بجوال آخر.

طريقة عمل الهاتف المحمول

عند تشغيل الجوال فإنه يستقبل إشارة تسمى بشيفرة نظام التعريف(SID) وهنا يتم التعرف بين جهاز الجوال ومحطة الإرسال، وبعد ذلك يقوم الجوال بمقارنة شيفرة التعريف الخاصة التي استقبلها ومقارنتها بتلك المخزنة في الجهاز، فإذا تمت المقارنة وتبين أنها نفس الشيفرة المتعارف عليها بين الجوال والمحطة، فإن الجوال يتعرف على الخلية التي سيتعامل معها.

ويقوم الجوال بعدها بإرسال طلب تسجيل إلى مكتب التحويلات (MTSO)الذي يمكن محطة الإرسال من تعقب مكان تواجد الجوال، وتخزن بيانات الموقع في قاعدة البيانات لاستخدامها في اللحظة التي يأتيك فيها

اتصال، وذلك لأنها تراقب دوما مكان الجوال والخلية التي تغطي الخدمة لتلك المنطقة المتواجد فيها الجوال.

فالمعلومات التي يحصل عليها مكتب التحويلات من الجوال عند تشغيله هي:

1. الرقم التسلسلي الالكتروني ESN وهو خاص بالجهاز الذي تستعمله، وكل جهاز له رقم يختلف عن الآخر .
2. رقم تعريف الجوال MIN .

ومن خلال الرقمين أعلاه يتم تحديد هوية الشخص، وعن طريق الخلايا المنتشرة في المنطقة فإنه يتم تحديد مكان أي جهاز نقال بدقة عالية على سطح الأرض.

التجسس على الهواتف المحمولة

الطرف الثالث او الشخص المهاجم او الجهات التي تقوم بالتجسس على الهواتف المحمولة غالبا ما تستخدم مجموعة طرق وأدوات مختلفة للحصول على المعلومات وفيما يلي أزكر بعضها:-

1. قائمة بجميع الاتصالات التي قمت بها، سواءً كانت صادرة أو واردة، مع مدة كل مكالمة وموعدها بدقة.
2. نسخة من جميع الرسائل القصيرة التي قمت بإرسالها أو استقبالها.
3. نسخة من جميع عناوين مواقع الإنترنت التي قمت بزيارتها من جهازك الجوال.
4. معرفة مكانك الحالي بدقة على الخريطة.
5. الاستماع إلى كل مكالماتك بحيث يكون طرفاً ثالثاً في أي مكالمة صادرة أو واردة.
6. الاستماع إلى أية أصوات بالقرب من هاتفك حتى ولو لم تقم بأي اتصال، كأن تكون في اجتماع مثلاً وهاتفك الجوال بجانبك، يستطيع عندها الاستماع إلى ما يدور في الاجتماع كاملاً دون علمك.

7. تشغيل الكاميرا الأمامية أو الخلفية والتقاط الصور والاحتفاظ بها.

8. استخدام أي برنامج على هاتفك والحصول على نسخة من أي بيانات مخزنة عليه.

9. حجب خدمة الاتصال عن المشتركين.

10. التشويش على المكالمات.

11. أخذ نسخة من البرامج والتطبيقات.

وسائل للحماية

معرفة كل هذه المعلومات التي ذكرتها أعلاه عن أي شخص أو جهه يعتبر كارثة وخرق كبير للخصوصية، لذلك كان من الضروري توضيح بعض الخطوات التي تساهم بشكل كبير في توفير الحماية والخصوصية للهاتف الجوال، ويجب أن يُعلم أن الوسائل المذكورة هنا لا توفر الحماية التامة، بيد أنها تقلل من المخاطر:-

1. يجب وضع كلمات المرور على الهاتف المحمول لحمايته من الآخرين.

2. عدم تمكين الأشخاص غير الموثوقون من الهواتف المحمولة.

3. عدم تلقي رسائل بلوتوث مجهولة المصدر أو مشبوهه.

4. إغلاق خاصية البلوتوث وتفعيلها فقط عن الحوجه.

5. ضبط الجهاز على وضع "غير قابل للإكتشاف" طوال الوقت وتحويله للوضع القابل عند الحاجه.

6. تجنب تأسيس الارتباط في مكان عام.

7. يجب اتعامل بحذر مع مهندسي وفنيي صيانة الجوال في حالة حاجة المحمول للصيانة.

8. تجنب التعامل مع محلات الصيانة الغير معتمدة.

9. استخدم برامج الحماية الخاصة بالجوال مثل Kaspersky Mobile Security .

10. في حالة الوجود ضمن بيئة سرية يجب إقفال المحمول أو سحب البطارية منه.

11. في حالة التعرض للهجوم يجب إخطار الشركة المقدمة لخدمات الاتصال.

12. يجب تبليغ الجهات ذات الصلة عند فقدان الهاتف المحمول أو فقدان بطاقة الاتصال.

13. في حالة بيع الأجهزة المحمولة يجب محوها من المتعلقات الشخصية كالأرقام والعناوين الالكترونية أو أي إعدادات أخرى مهمه.

14. إذا كنت تقوم بأمر حساس على الجوال، كالكشف على حسابك المصرفي، أو تسديد إحدى الدفعات، فلا تستخدم شبكة «واي فاي» المجانية الموجودة في المقهى، أو غيرها من الأماكن، بل استخدم «واي فاي» الخاصة بك في المنزل المحمية بكلمة مرور، أو شبكة الجوال، لتفادي ما يسمى بهجوم الشخص الوسيط، حيث يجري اعتراض حركة الاتصال، أما مزاوجة الجوال مع جهاز آخر يدعم «بلوتوث»، كسماعة الرأس مثلا، فهذا يعني أن بمقدور أي جهاز يكتشف جهاز «بلوتوث» آخر، بمقدوره إرسال رسائل متطفلة، أو القيام بأمور قد تؤدي إلى دفع رسوم إضافية، أو التلاعب بالمعلومات، أو إفسادها، أو سرقتها، عبر هجمات تدعى «بلوسنيرينغbluesnaring »، أو الإصابة بعدوى الفيروسات. وبعبارة أخرى قم بتعطيل «واي فاي» و«بلوتوث»، إلا إذا كنت بحاجة ماسة إلى استخدامهما.

15. علِّم على الشريحة ماديًا بالرسم عليها، وعلي بطاقة الذاكرة الإضافية، والبطارية، والهاتف برمز مميز ويصعب على الغرباء ملاحظته (ارسم علامة صغيرة، أو رسمة، أو أرقامًا وأحرف، أو جرب استخدام قلم الأشعة فوق البنفسجية الذي لا يظهر حبره في الضوء العادي). ضع ملصقات ضد التلاعب أو شريطًا لاصقًا على أطراف الهاتف. سيساعدك ذلك في معرفة ما إذا عُبث بأحد تلك الأشياء أو إذا استُبدلت مثلًا: سيكون الملصق ممزقًا، أو منحرفًا عن مكانه الأصلي، أو سيخلف بقايا واضحة.

16. تأكد من أنك تعرف البيانات المخزنة على شريحتك، وعلى بطاقات الذاكرة الإضافية، وعلى ذاكرة هاتفك. لا تخزن معلومات حساسة على الهاتف. إن احتجت إلى تخزين مثل تلك المعلومات فضعها في بطاقات ذاكرة خارجية يسهل التخلص منها عند الحاجة. لا تضع التفاصيل الهامة في ذاكرة الهاتف الداخلية.

17. حافظ على شريحتك وبطاقة الذاكرة الإضافية (إن كنت تستخدمها)، فربما تحتوي معلومات حساسة مثل تفاصيل الاتصالات والرسائل القصيرة. على سبيل المثال، تأكد من عدم تركها في محل الصيانة عند إصلاح هاتفك.

18. الرقم التسلسلي المكون من 15 رقمًا أو رقم IMEI يساعدك في التعرف على هاتفك، ويمكن الوصول إليه بطلب الرقم #06 في معظم الهواتف، أو بالنظر خلف بطارية هاتفك، أو بتفقد إعدادات الهاتف. احتفظ بهذا الرقم وأبقه بعيدًا عن هاتفك، فالرقم يساعد في تتبع ملكيته وإثباتها سريعًا في حال سرقته.

19. ضع في الحسبان محاسن تسجيل هاتفك لدى مقدم الخدمة ومساوئه. إذا أبلغت عن سرقة هاتفك فسيتمكن مقدم الخدمة من منع استخدام هاتفك، لكن تسجيله يعني أن استخدام هاتفك مربوط بهويتك.

الثغرات الأمنية للهواتف المحمولة

تحتوي منظومة الأمان في الهواتف المحمولة على مجموعة من نقاط الضعف التي قد تساعد على إختتراقها ومنها:-

1- لو افترضنا أن شخصاً ما فقد سماعة الهاتف الجوال المزود بتقنية البلوتوث فإن من يجد هذه السماعة يمكنه التنصت على اتصالات صاحب الهاتف الجوال؛ وذلك لأنه قد سبق تأسيس ارتباط بين الجوال والسماعة، مما جعل السماعة تحوز المعلومات اللازمة لإنشاء الاتصال مع الجوال في أي وقت، كما أن

هذه المعلومات تمكن السماعة من فك التشفير الذي يستخدمه الجوال أثناء الاتصال.

2- كما يمكن استغلال السماعة بجعلها تنتحل شخصية الهاتف الجوال لتتصل بالحاسوب المحمول لتحقيق مزيد من الاختراق وجمع مزيد من المعلومات عن الشخص المستهدف.

كما بإمكان شخص ما لديه جهاز مزود بالبلوتوث أن يذهب بالقرب من شخص آخر لديه جهازاً مزوداً بالبلوتوث، وإعداداته على وضع التشغيل، وينشئ معه اتصالاً يقوم من خلاله بتحميل فيروسات وبرامج تجسس.

3- يضاف إلى البلوتوث إمكانية اختراق الهاتف الجوال للشخص المستهدف من خلال الانترنت عند تصفحه لأي موقع أو فتحه لإيميله من خلال جواله، وما ينطبق على الهاتف الجوال ينطبق على الكمبيوتر المحمول فيما يتعلق بخطورة البلوتوث أو الإنترنت.

4- التمكين الدائم لخدمة الحزمة البرمجية .

5- تمكين خدمة الموجات الحمراء.

6- التمكين الدائم لخدمة المؤتمرات الفيديوية.

7- عدم تمكين خدمة التعرف على الأماكن المرتبطة بالاقمار الاصطناعية إلا عند الحوجه لها.

برامج التجسس الخفية

ظهرت في الأونه الاخيرة العديد من البرامج المتخصصة في التجسس على الجوال Spyware إضافة للعديد من الفيروسات الشبيهة بفيروسات الكمبيوتر سواء للحاسب وبرامج حصان طروادة Trojan Horse وهي برامج تتظاهر بكونها ذات أغراض مفيدة وعند تحميلها تُكشف حقيقتها بأنها ذات أغراض خبيثة.

بوسع الفيروسات أو برامج التجسس وبرامج حصان طروادة أن تقدم لأي شخص عادي إمكانية التجسس

على أي هاتف جوال بتركيب برنامج تجسسي مخفي فيه، لا يستطيع صاحب الجوال اكتشاف هذا البرنامج بسهولة ولا رؤيته من قائمة البرامج المثبتة في الجهاز، هذه البرامج – على بساطتها – تقدم الكثير من المعلومات للجهات التي تقوم بالتجسس.

الهجوم على الهواتف المحمولة

الهواتف الذكية ليست مجرد أجهزة ذكية فحسب، بل إنها تعتبر حواسيب شخصية أيضا وهي تتيح حفظ الصور عليها، والدخول إلى البريد الإلكتروني، وتلقي الرسائل النصية وإرسالها، ومن مخاطرها على المتصفح انها تضعه على مسافة نقرة واحدة من مواقع الشبكة الخبيثة والضارة، كما انها تتعرض لشتى الاخطار، فخلافا للحواسيب المكتبية، أو حتى الكومبيوترات المحمولة (لابتوب)، يمكنها مثل الاجهزة الجوالة الأخرى أن تسقط بسهولة من الجيب، أو المحفظة، أو يجري نسيانها في سيارات التاكسي، أو تسرق لدى وضعها على الطاولات .

إحتياطات السلامة

ينبغي أن يقتصر استخدام الموبايل علي الأمور المهمة والطارئة فقط ، لا أن يكون وسيلة للمناقشات الطويلة، ويجب تكملة المناقشة علي تليفون أرضي قريب .

ينبغي ألا تزيد مدة المكالمة علي دقيقتين .

ينبغي ألا يوضع الموبايل في الجيب سواء في الجاكيت أو البنطلون .

ينبغي ألا يوضع الموبايل في الحزام أو في غلاف به معدن، لأن ذلك يزيد من نسبة امتصاص الموجات الكهرومغناطيسية .

يجب ارتداء سماعات من نوعيات معينة عند الكلام بحيث يظل الموبايل بعيدا عن الرأس والجسم .

حاول استخدام الرسائل بدلا من المكالمات بقدر الإمكان .

ينبغي عدم استخدام المحمول في الأماكن المغلقة مثل المصعد أو داخل السيارة. حيث تخرج من التليفون المحمول آنذاك موجات أقوي لكي تتم عملية الاتصال , ويتم امتصاص جزء كبير منها من خلال جسم الإنسان وخلاياه .

لا تحاول استخدام الموبايل عندما تكون إشارة الشبكة علي أول شرطة لنفس السبب السابق .

عندما تشتري موبايل ينبغي أن تبحث في كتالوج التشغيل الخاص به عما يسمي SAR وهو اختصار Specific Absorption rate أي نسبة الامتصاص النوعية التي تحدث من خلال امتصاص الجسم لما يصدر عن الموبايل من طاقة وإشعاع، وكلما كانت هذه النسبة أقل، كان ذلك أفضل .

تجنب أخذ المحمول معك إلي الفراش أو تحت المخدة التي تنام عليها، لأن الموجات المنبعثة منه قد تؤثر علي كهرباء المخ، مما يسبب اضطراب النوم، صداعا، عدم تركيز، نسيانا..الخ

مراعاة الامان:

ينبغي الحد من استخدامه أثناء القيادة بقدر الإمكان والتركيز على الطريق للمحافظة علي حياتك وحياة من معك إلا في حالة وجود السماعة الخارجية.

نبرة الصوت:

ينبغي أن تكون نبرة صوت الشخص المتحدث، وصوت الهاتف نفسه هادئة لا تسبب إزعاج لغيرك. فالهاتف له ميكروفون حساس قادر علي نقل الأصوات الهامسة وليست المنخفضة فقط. كذلك يجب مراعاة استخدام (الذبذبات) بدلاً من الرنين وخاصة أثناء الاجتماعات والأعمال الهامة أو في وجود شخص مريض أو نائم.

المسافة والبعد:

لأي شخص منا حيز شخصي خاص به وهو المكان الذي يشغله، وهنا الحيز لا بد وأن يضمن إحساس الإنسان بالأمان والهدوء وخاصة في الأماكن المزدحمة. وعندما يتعدي شخص حدود منطقته هذه ليخترق ملكية الآخرين فسوف يصيبهم بعدم الراحة والارتياح. بتجاهل الحيز الشخصي للآخرين والتظاهر بالتناسي ترفع شعار الأنانية وتجبر الآخرين على عدم احترامك.

الخصوصية:

السبب الرئيسي وراء اختراع الهاتف المحمول هو ضمان سير الأعمال الهامة علي ما يرام في الوقت المناسب لها، لأن في بعض الأعمال ينبغي اتخاذ قرارات فورية وحازمة لا تتطلب أي تأجيل. وبما أن أي معلومة تتصل بالأعمال هامة فيتحتم أن تحاط بشيء من السرية أو الخصوصية. ولا تنس ان شعار الهاتف المحمول هو" خير الكلام ما قل ودل لإبلاغ الأمور الهامة بإيجاز، فهو غير مخصص لإدارة شئون المنزل أو الأسرة أو الشجار في أمور العمل.

الخاتمة

تخلص هذه الدراسة على أنه وبالرغم من عدم إغفال المميزات العديدة التي توصلت لها ثورة المعلوماتية في الهاتف الجوال إلا أنه لا يمكن أيضاً تجاهل المخاطر الأمنية الحقيقية التي تسببت بها على الأفراد والمؤسسات والمجتمعات بصورة عامة لذلك أوضحت في هذه الورقة البحثية مجموعة من التدابير الأمنية التي تساعد الجميع على الحفاظ خصوصياتهم من المهاجمين والمخربين الذين يستخدمون مجموعة من الحزم البرمجية والأدوات لمهاجمة هذه الخصوصية.

ختاماً لم يصبح الهاتف المحمول بعد الآن مجرد هاتف للمكالمات وتبادل الرسائل النصية إذ أصبحت الآن مجموعة كبيرة من التطبيقات والخدمات متاحة عن طريقه مثل خدمات الوصول للحسابات البنكية وبعض تطبيقات التجارة الالكترونية بالاضافة الى استخدامها في دفع فواتير الهواتف الأرضية والمياه والكهرباء والانترنت والمخالفات المرورية.

لذلك تناولت هذه الورقة اهمية إستمرار خدمة الهواتف المحمولة والمخاطر التي تتعرض لها المعلومات وهي في طريقها من المرسل الى المستقبل ومدى أهمية هذه المعلومات بالنسبة لخصوصية الأفراد والمؤسسات واهم الطرق لحماية المعلومات في الهاواتف النقالة.

المراجع

http://defense-arab.com/vb/showthread.php?t=28045 2/3/2011

الموقع العربي للموسوعة الحرة 13/2/2011

http://fashion.azyya.com/154787.html 16/2/2011

https://securityinabox.org/ar/chapter_09_02_1 11/3/2011

https://securityinabox.org/ar/glossary 11/3/2011

http://www.ictqatar.qa/ar/regulatory-authority/consumers/protecting-your-mobile-phone-spam-and-scam 12/3/2011

http://ejabat.google.com/ejabat/thread?tid=2960057e9ce88266 /2/2011