٣- هجمات الاحتمالات الكاملة Brute Force Attacks : تعتبر من أخطر الطرق المتبعة لكسر كلمات السر، حيث أنها تقوم بتجربة جميع الاحتمالات التي يمكن استخدامها وبجميع التراتيب والتباديل للمفاتيح الخاصة بلوحة المفاتيح ، فتستخدم مزيجاً من الأحرف والأرقام والعلامات والرموز الخاصة. بالطبع فإن تلك العملية قد تستغرق وقتاً طويلاً ، ولكن في النهاية فإن هذه الطريقة قادرة على كسر كلمة السر.
نصيحة: كلمة السر يجب أن تكون طويلة قدر الإمكان وتحوي أحرف كبيرة وصغيرة وأرقام ورموز خاصة، كما يفضل تغيير كلمة السر بين فترة وأخرى.

٤- الصيد Phishing : من الطرق التي بدأت بالانتشار في وسط الإنترنت وكانت سبباً في العديد من عمليات سرقة معلومات الدخول إلى البريد الالكتروني للمستخدم. تقوم تلك الآلية على مبدأ خداع المستخدم واستدراجه للنقر على رابط ما أو صندوق حوار عن طريق إيهامه بعملية ربح أو هدية مجانية أو غيرها من الطرق الأخرى، وعند النقر على الرابط يطلب منك بريدك الالكتروني وكلمة السر الخاصة بك، وقد تقوم بعض المواقع بتزوير واجهة بريدك الإلكتروني أو تغيير بعض الأحرف في عنوان الموقع الخاص بخدمة البريد الإلكتروني في محاولة لإيهامك بأنك قد قمت بعمل تسجيل خروج من بريدك الإلكتروني! فتقوم بإدخال كلمة السر من جديد التي ترسل مباشرة للمخترق على الطرف الآخر!.
نصيحة: لا تنقر على أي رابط مجهول ولا تعرف مصدره، ولا تعطي كلمة السر الخاصة بك لأي شخص أو موقع مهما كانت الأسباب! فحتى مدير الأنظمة في شركتك لن يحتاج منك كلمة السر الخاصة بك لانه قادر على تغييرها بكل بساطة!

٥- التسلل من فوق الكتف! Shoulder surfing: يبدو المصطلح مضحكا عند ترجمته إلى العربية ولكن الأمر يتعلق بمن يتسللون خلسة من وراء ظهرك أثناء إدخالك لكلمة السر ويحاول استراق النظر إلى لوحة المفاتيح أو النظر إلى قصاصات الورق التي على مكتبك والتي يستخدمها بعض المستخدمين لكتابة كلمات السر عليها!
نصيحة: حاول إدخال كلمة السر بسرعة ودون النظر إلى لوحة المفاتيح، ولا تكتب كلمات السر الخاصة بك على أي أوراق وتلصقها على الشاشة التي أمامك!.

نصائح حول طرق اختيار كلمات السر القوية

عند اختيارك كلمة سر قوية فإنك توفر الحماية لك ولزملائك أيضاً، فعند اختراق أحد الأجهزة في العمل مثلا فإن جميع الأجهزة الأخرى قد تصبح معرضة للخطر نتيجة لهذا الاختراق الأمني.
هذه بعض النصائح المفيدة لكيفية أختيار كلمة السر الخاصة بك:
١- استخدم الأحرف الكبيرة والصغيرة Upper and Lower cases.
٢- استخدم الأرقام وعلامات الترقيم في كلمة السر.
٣- اجعل كلمة السر طويلة قدر الإمكان، ويفضل أن تكون ما بين ٨ إلى ٢٠ حرفاً.

٤- استخدم الرموز الخاصة مثل ! @ # $ ٪ * - + = ( ) , < > : " '
٥- تمرن على طباعة كلمة السر بشكل سريع لتتجنب عمليات استراق النظر أثناء إدخالك لها.
٦- لا تستخدم كلمات قاموسية أو معروفة، وحاول استخدام جملة معينة بدلا من الكلمات. هذه طريقة جيدة تشرح لك هذه الطريقة:
لنأخذ الجملة الإنجليزية : I Love Ketchup على سبيل المثال. قليل من التعديل باستبدال حرف e بالرقم 3 تصبح:
I Love K3tchup
الآن دعنا نضيف الرمز الشهير الذي نستخدمه في برامج المحادثة والذي يرمز للإبتسامة " :) "إلى آخر الجملة، فتصبح عندها:
I Love K3tchup:)
نقوم بحذف الفراغات فتصبح لدينا كلمة المرور القوية ILoveK3tchup:)