شنبه 24 آذر 1386 - 08:44

چطور کلمه عبور خود را حفظ کنیم؟

حتما شما هم این جمله را از مسئول کامپیوتر یا شبکه یا افراد متخصص در کامپیوتر شنیده‌اید:

"کلمه عبور خود را به دیگران ندهید" یا جمله‌هايي شبيه به اين مبني بر حفظ و نگهداري از كلمه عبور. دليل اين همه اصرار و جمله‌هاي تكراري چيست؟ و چرا ما بايد كلمه عبور خود را از همكار يا هر فرد ديگري پنهان نگهداريم؟

بدون شك، تمام كاربراني كه تا به حال با كامپيوتر كار كرده‌اند،[چطور با كامپيوتر كار كنيم؟] مي‌دانند كه فايل‌ها، تنها اجزاء داراي ارزش در كامپيوتر هستند [چند نكته درباره كامپيوتر] كه در صورت از بين رفتن، شايد هرگز قابل برگشت نباشند. به طور كل، انواع مختلف فايل‌هايي كه يك كاربر در طول ماه‌ها و سال‌هاي گذشته براي خود توليد يا جمع‌آوري مي‌كند، به عنوان سرمايه‌ايي براي او محسوب مي‌شود.

چنانچه اين فايل‌ها مربوط به محيط كار يا پروژه‌هاي كاربر باشد، ادامه كار او به آنها بستگي دارد و چنانچه مربوط به مسائل شخصي باشد، مي‌تواند زندگي و آرامش شخص را به خطر بياندازد.

همانطور كه اكنون حفظ رمز كارت‌هاي اعتباري

براي همه افراد ضروري
است (به دليل ارتباط
مستقيم با سرمايه)
بديهي است با بالا رفتن
ارزش اطلاعات ديجيتال،
لزوم حفظ و نگهداري از
رمز نيز امري واجب
خواهد شد.
با توجه به مسائل فوق،
نگهداري، حفظ و انتخاب
يك رمز خوب براي هر
كاربر امري لازم و ضروري
به نظر مي‌رسد و با توجه
به افزايش دستگاه هاي
ديجيتال و لزوم انتخاب
رمز براي هر كدام از آنها
به نظر مي‌رسد در آينده
تمامي افراد، تمايل به
حفظ و نگهداري رمز را
در خود احساس
مي‌كنند. به همين منظور
لازم است كه اطلاعاتي
هرچند كم در اين زمينه
دارشته باشيم.
اهميت حفظ رمزها
توسط صاحبان آنها به
حدي است كه اكنون
توصيه‌هاي بسياري در
اين زمينه مي‌شود تا
كاربران را مجاب به دقت
بيشتر در اين راستا و
همچنين فراگيري
ريزه‌كاري‌هاي اين امر
كند. اكتشاف رمز و به
دست آوردن رمز ديگران
يكي از دغدغه‌هاي
هكرها بوده تا با استفاده
از آن بتوانند به اطلاعات
شخصي يا كاري يك
كاربر دست يافته يا از
طريق آن وارد يك شبكه
محلي شوند. اصولا چهار
روش شناخته شده براي
به دست آوردن رمز
ديگران وجود دارد كه در
صورت آشنايي كاربران با
آنها، مي‌شود درصد
بسيار زيادي از آن را
كاهش داد. اين چهار
روش به شرح زير
هستند:

1- Passive Online Attacks: در این روش هکرها از نرم‌افزار یا سخت‌افزارهاي جاسوسي يا Sniffer ها استفاده مي‌کنند. به این ترتیب که این نرم‌افزار یا سخت‌افزار با قرار گرفتن بر روي شبکه، اطلاعات در حال انتقال بر روي سیم‌ها را Sniff کرده و براي هکر ارسال مي‌کنند.(سخت‌افزارهاي Sniffer در کنار کابل شبکه (کابل‌هاي سیمي) قرار گرفته و اطلاعات داخل آن را مي‌خوانند ولي نرم‌افزارها با نصب بر روي يك کامپیوتر شبکه این کار را انجام مي‌دهند). طبق آخرین اخبار غیر رسمي، سخت‌افزار Sniffer کابل فیبر نوري با قیمت 45000 دلار در آمریکا ساخته شده است.

2- Active Online Attacks: این روش در واقع حدس زدن رمز کاربران است که روش تجربي و با توجه به فرهنگ و ذهنیات فرد است. به طور معمول کاربران از مبتدي تا حرفه‌اي سعي مي‌کنند رمزي را براي خود در نظر بگیرند که به راحتي بتوانند آن را در خاطر نگهدارند. به همین دلیل اکثر کاربران از موارد آشنا نظیر شماره شناسنامه، نام فرزند، نام همسر و ... که همگي قابل حدس زدن مي‌باشند را به عنوان رمز خود در نظر مي‌گیرند. کاربران زرنگ‌تر از ترکیب آنها استفاده مي‌کنند که یافتن و حدس زدن آن کمي مشکل‌تر خواهد بود.

هکرها نیز با توجه به

اين اصل كه كارايي بسياري نيز براي آنها دارد، ابتدا اطلاعات پرسنلي افراد را يافته و با آنها به حدس‌زني رمز مي‌پردازند.

-Offline Attacks 3:

در اين روش از ابزار نرم‌افزاري براي يافتن رمز استفاده مي‌شود. اين ابزارها معمولا بر دو نوع هستند:

الف - Dictionary Attack: ابزارهاي اين روش، با كمك گرفتن از ذهن هكر، به يافتن رمز در كلمات لغت‌نامه مي‌پردازند. براي اين كار حتي از لغت‌نامه‌هاي غير انگليسي نيز استفاده مي‌شود (لغت‌نامه فارسي نيز براي اين موضوع درست شده است)

ب - Brute Force: در اين روش نرم‌فزار ابتدا تعداد حروف رمز را با كمك هكر (يا بدون كمك) يافته و با استفاده از حروف و كلمات پيشنهادي هكر، به صورت منظم و يك به يك با جاي‌گذاري آنها ، سعي در يافتن رمز مي‌كند(در اين روش به دليل تعداد بسيار بالاي حروف و اعداد، ممكن است زمان بسياري نياز داشته باشد و هرچه رمز قوي‌تر و پيچيده‌تر باشد، زمان بيشتري لازم دارد).

در اين روش بديهي است كه انتخاب رمز مناسب و قوي مي‌تواند به شكست اين نرم‌افزار بيانجامد. در مواردي كه رمز قوي و مناسب است براي پيدا كردن آن،حتي ممكن است كامپيوتر احتياج به چندين سال زمان براي يافتن آن

داشته باشد که عملا غیر قابل استفاده خواهد بود.

4- Non Electronic Attacks: در این روش از راه‌هاي غير معمول و غيركامپيوتري براي يافتن رمز ديگران استفاده مي‌شود. برخي از این روش‌ها عبارتند از:

الف- نگاه کردن به کي‌بورد هنگام تایپ کاربر بدون اینکه او متوجه شود (معمولا افرادي که از تبحر خاص در تایپ برخوردارند یا چشمان تیزي دارند به راحتي مي‌توانند حروفي که تایپ مي‌شوند را ببینند)

ب - از پشت سر فرد نگاه کردن

ج-کاغذ فسفري: با دادن يك كاغذ مخصوص فسفري به کاربر بدون اینکه او متوجه شود، دستانش به فسفر آغشته شده، سپس بر روي کي‌بورد اثر کلماتي که تایپ مي‌کند، برجا خواهد ماند. البته این اثرات در حالت عادي غير قابل رویت هستند و با نور مخصوصي که به آنها تابیده مي‌شود، قابل رویت خواهند بود. به این ترتیب فرد مي‌تواند متوجه رمز کاربر شود یا حداقل بخش عمده‌اي از آن را به دست آورد.

د - مهندسي اجتماعي: هکرها اعتقاد بسیاري به این مهندسي دارند. در این روش با استفاده از فرهنگ، ذهنیات، کمبودهاي روحي و ... افراد مختلف، اطلاعات مهمي را به دست مي‌آورند. به واقع در این روش که بسیار نیز موثر است، با ترفندهاي

مختلف، اطلاعات فرد را از خود او يا اطرافيانش به دست مي‌آورند. در اين روش بيشتر كه بر روي مسئول شبكه يا افراد مهم انجام مي‌شود و به جاي استفاده از ابزار، سعي مي‌شود با روش‌هاي مختلف گفتاري، رمز يا اطلاعاتي كه منجر به لو رفتن رمز مي‌شود را از زبان خود فرد بيرون كشيد.

علاوه بر روش‌هاي فوق كه به صورت دسته‌بندي شده وجود دارد، چند روش كه هنوز دسته بندي نشده نيز وجود دارد كه به معرفي آنها مي‌پردازيم:

1- Key Loggers: اين نوع نرم‌افزارها با قرارگيري بر روي يك سيستم، كليه استفاده‌هاي كاربر از ماوس و كي‌بورد را ضبط كرده و براي هكر ايميل مي‌كند. در اين روش حتما مي‌بايست نرم‌افزار بر روي كامپيوتر شما نصب شود پس دقت كنيد هيچ نرم‌افزاري را بدون شناسايي و نوع عملكرد بر روي كامپيوتر خود نصب نكنيد.

2- Fishing: در اين روش، صفحه‌اي مشابه يكي از سايت‌هاي معتبر جهان ساخته و براي شما ارسال مي‌شود يا اينكه شما را تشويق به ثبت نام براي شركت كردن در يك قرعه‌كشي بزرگ مي‌كند و شما نيز بدون توجه،تمام اطلاعات خود را وارد مي‌كنيد. توجه داشته باشيد حتي اگر اين كار را انجام مي‌دهيد، از رمز ايميل يا رمزهاي مهم خود در اين صفحات استفاده نكنيد

و به صفحاتي كه از شما اطلاعات مي‌خواهند به راحتي پاسخ ندهيد.

در ادامه چند پيشنهاد براي حفظ رمز و نهايتا حفظ اطلاعات به شما پيشنهاد مي‌كنم،

اميدوارم كه مفيد باشد:

-1 انتخاب رمز قوي: به راستي چه رمزي قوي و مناسب است؟ پيشنهاد من به شما انتخاب رمزي حداقل 8 حرفي با تركيبي از حرف، عدد و يكي از كاراكترهاي خاص (@-$=% و ...) است. كاراكتر خاص را فراموش نكنيد زيرا باعث مي‌شود نرم‌افزارهاي Brute Force از يافتن رمز شما عاجز شوند.

-2 استفاده از دو روش براي شناسايي: در سيستم خود و براي ورود از دو روش شناسايي استفاده كنيد مثلا استفاده از كارت هوشمند و رمز معمولي به صورت سري كه باعث مي‌شود ورود به محوطه شخصي شما بسيار سخت شود. اين روش معمولا هزينه چنداني نيز براي شما ندارد.

-3 استفاده از تجهيزات بيومتريك: تجهيزات بيومتريك، تجهيزاتي هستند كه از مشخصات منحصر به فرد فيزيك شما استفاده مي‌كنند مانند اثر انگشت، اثر شبكيه چشم صدا يا ... . اين موارد چون تقريبا در جهان منحصر به فرد است، غير قابل تقلب و سوء استفاده است. در حال حاضر بهترين روش شناسايي افراد در جهان همين روش است و تنها ضعف وارده به آن، قيمت بالاي آن است

ولي به نظر مي‌رسد
آينده از آن اين
تكنولوژي است.
با توجه به موارد ذكر
شده فوق، با كمي دقت
مي‌توانيم علاوه بر حفظ
اطلاعات شخصي و كاري
خود، از عواقب خطرناك
لو رفتن آن نيز جلوگيري
كنيم.
همشهري آنلاين - محمد
رسولي