در دنیای مجازی آن چه مهم است ،حفظ امنیت و بالا بردن آن با چند روش ساده می باشد.برای آنکه بخواهیـــــم از دست کلاه سیاهان فرار کنیـــــــم به روش های زیر به دقت توجه کنیم

انتخاب نکردن یک رمز برای همه حساب ها!

درست است که استفاده از یک رمز واحد برای انواع حساب های کاربری و به خاطر سپردن آن بسیار آسان است اما به همان آسانی نیز دیگران می توانند از ما سوءاستفاده کنند. اگر پسورد ایمیل یا یکی از حساب های کاربری ما دست یک هکر بیفتد، شک نکنیم او آن رمز را در سایت های دیگر نیز امتحان خواهد کرد و می تواند به راحتی به دیگر حساب های کاربری ما دسترسی پیدا کند .بنابراین، هرگز از یک رمز واحد برای همه حساب های خود استفاده نکنیم.

انتخاب رمز قوی و غیر قابل حدس!

در قسمت اول: نباید برای همه ی حساب های کاربری خود رمز یکسانی انتخاب نمائیم در این جا آن چه مهم است انتخاب رمزی که تشکیل یافته از اعداد و حروف باشد و حدس آن توسط دیگران تقریبا صفر باشد.علاوه بر داشتن رمزهای متفاوت، باید مطمئن شویم که رمز عبور ما قوی و غیر قابل حدس زدن نیز هست.رمز خود را در مدت های معین تغییر دهیم تا امنیت آن بالا رود مثلا هر ۴ ماه یک بار. در صورت فراموشی رمز می توانیم آن ها را در یک فایل اکسل ذخیره و یا از نرم افزار Manage password استفاده نمائیم.

رمز دوم برای حساب خود

برا ی افزایش بیشتر امنیت بهتر است که ما برای حساب کاربری خود علاوه بر یک رمز ،رمز دومی هم تدارک ببینیم.این امکانات معمولا در گوگل و .. نیز سایر حساب های کاربری فعال می باشد.رمز دوم می تواند از حروف نوشتاری و یا صوتی باشد.خوب است که برای خود یک لایه حفاظتی دیگر ایجاد نمائیم.

اطلاعات کم=امنیت بالا

خیلی از افراد به محض حضور در شبکه های اجتماعی مانند فیس بوک و ... همه ی اطلاعات خود را اعم از منزل ، محل کار ، شماره موبایل و آنچه را که به آن علاقه دارند را در این مکان ها قرار می دهند. و این چیزی جزء نا امنی برای ما بوجود نمی آورد.حتی از قرار دادن آن ها در صفحات دوستانمان خودداری کنیم.هکر ها منتظر اطلاعات ما هستند تا رمز ما را از بین اطلاعاتمان کشف و....
به همین منظور دقت کنیم تا از دادن اطلاعات زیاد در فضای مجازی خودداری نمائیم.

به کامپیوتر و مرورگر خود توجه کنید!

مهم نیست از چه سیستم عاملی استفاده می کنیم، باید همیشه آنتی یروس آپ دیت روی سیستم خود نصب کنیم. همیشه به روز بودن در مورد سیستم عامل و مرورگر، باعث می شود تا بهترین سرویس های امنیتی را نیز داشته باشیم. به طور مثال، گوگل بسیار تاکید دارد از جدیدترین نسخه مرورگر کروم استفاده کنیم.

حفظ امنیت اتصال وایرلس

طریقه اتصال به اینترنت نیز باید امن باشد. برای اطمینان از این امر، شبکه بی سیم خود را رمزگذاری کنیم و تنظیمات پیش فرض SSID (نام شبکه) را تغییر دهیم. هنگام اتصال به شبکه وای فای عمومی، مراقب اطلاعاتی باشیم که از طریق آن منتقل می کنیم. به طور مثال، می توانید از نرم افزار HotSpot Shield استفاده کنیم. این برنامه امنیت شبکه مود نظر را مشخص می کند.

سایتی مطمئن برای خرید شما

اگر قصد خرید اینترنتی داریم، سعی کنیم پیش از ورود به سایت و وارد کردن رمز عبور کارت خرید خود، مطمئن شویم که نشانی HTTPS دارد. حسابی هم مراقب میزان پول خود در حسابمان باشیم که اگر کوچک ترین تغییری در آن ایجاد شد، متوجه شویم. بعلاوه، پیش از خرید از قانونی و مطمئن بودن سایت اطمینان حاصل کنیم.

تفکر+کلیک بر روی لینک ها

کلیک کردن روی لینک های مختلف یکی از اصلی ترین کارهایی است که در اینترنت صورت می گیرد. اما توصیه می کنیم، مراقب لینک هایی باشیم که کلیک می کنیم. ساخت وب سایت های تقلبی که شبیه سایت رسمی بانک هاست برای هکرها بسیار آسان است. اگر به اشتباه وارد این سایت های دروغین شویم، با ورود رمز عبور خود در واقع همه اطلاعات حساب خود را در اختیار سوءاستفاده کننده های اینترنتی قرار داده ایم.

برای امنیت بیشتر خود، به ویژه وقتی ایمیلی از یک شرکت یا وب سایت دریافت می کنیم، قبل از اطمینان از سالم بودن آن لینک های موجود را باز نکنیم. در فیس بوک نیز پیغام های غریبه را باز نکنیم. اگر دوستان در فیس بوک بخواهند عکس هیجان انگیزی را با ما به اشتراک بگذارند، لینک آن را برایتان ارسال نمی کنند. حواس خود را جمع کنیم.

ایجاد رمز عبور برای موبایل خود

گوشی های هوشمند یک کامپیوتر تمام عیار برای خود هستند و کاربران اطلاعات شخصی زیادی را روی آن ذخیره می کنند. بنابراین، حفظ امنیت گوشی بسیار اهمیت دارد. برای این کار باید برای گوشی خود رمز عبور تعیین کنید. کابران اندروید همچنین باید از نرم افزارهای امنیتی و ضدویروس نیز استفاده کنند.

نکته آخر

در آخر به همه ی وب گردان عزیز توصیه می کنیم که حواس خود را در زمان چرخ زدن و وب گردی در اینترنت و سایت های مختلف جمع کنند و همه ی موارد امنیتی که ذکر شد را رعایت نمایند تا دچار پشیمانی در فضای مجازی نشوند.