مخاطرات سایبری
پدافند غیرعامل

مدیریت آمار، فناوری اطلاعات

رمز عبور مناسب

کلمه عبور پیچیده

با گره خوردن زندگی امروز افراد با فضای مجازی و زندگی دیجیتال، اطلاعات فردی و ابزارهای ارتباط مالی از اهمیت ویژه برخوردار است و بی احتیاطی در این موارد میتواند صدمات جبران ناپذیری مانند از بین رفتن همیشگی اطلاعات یا ضررهای هنگفت مادی و معنوی را به همراه داشته باشد، بنابراین رعایت اصول اولیه امنیت اطلاعات در مقابل افرادی که قصد نفوذ و آسیب رساندن و سوء استفاده از این اطلاعات را دارند، از ضروریات اولیه استفاده از این فضا می باشد.

نیاز به داشتن یک رمز عبور امن و غیر قابل حدس(Password Complexity)

افراد برای انجام هر کاری یا استفاده از هر نوع خدماتی ابتدا باید توسط سیستم مشخصی **احراز هویت (Authentication)** شوند و معمولا هر احراز هویت نیاز به دو عنصر دارد، **نام کاربری و رمز عبور (Username & Password).**

بنابراین رمزهای عبور حساب های کاربری، ایمیل ها و کارت های اعتباری و ...، اولین و مهمترین سد دفاعی در برابر هکرها و یا هر عامل یا فردی که قصد نفوذ و آسیب رساندن و سوء استفاده از اطلاعات افراد را داشته باشد، هستند. در نتیجه برای جلوگیری از این امر، به کلمه عبور امن و غیرقابل حدس نیاز است. اما سوالی که مطرح می شود اینست که چگونه یک کلمه عبور امن ایجاد نمود و در گام بعدی برای نگهداری آن چه اقداماتی باید انجام داد.

ویژگی های یک رمز عبور مطمئن و مناسب

رمزهای عبور ساده که از ترتیب حروف و یا اعداد مانند qwerty، abc۱۲۳ یا ۱۲۳۴۵۶ مورد استفاده کاربران قرار می گیرند جزء اولین گزینه هایی هستند که هکر ها نسبت به آزمایش آنها اقدام می کنند. بنابراین برای ساختن یک رمز عبور مطمئن و مناسب بهتر است که بدانیم یک کلمه عبور امن چه مشخصاتی دارد و چگونه باید ساخته و نگهداری شود. برای ساختن یک رمز عبور مناسب، تکنیک های متفاوتی وجود دارد. با یک جستجوی ساده در اینترنت، میتوانید با بیشتر این روشها آشنا شوید، اما به طور کلی کارشناسان مسائل امنیتی همواره تاکید میکنند یک رمز عبور مناسب باید **ترکیبی از حرف کوچک، بزرگ، اعداد وعلایم** باشد.

البته شما میتوانید روش خاص خود را هم داشته باشید، اما بد نیست که با برخی از روشهای رمزگذاری معمول نیز آشنا شوید:

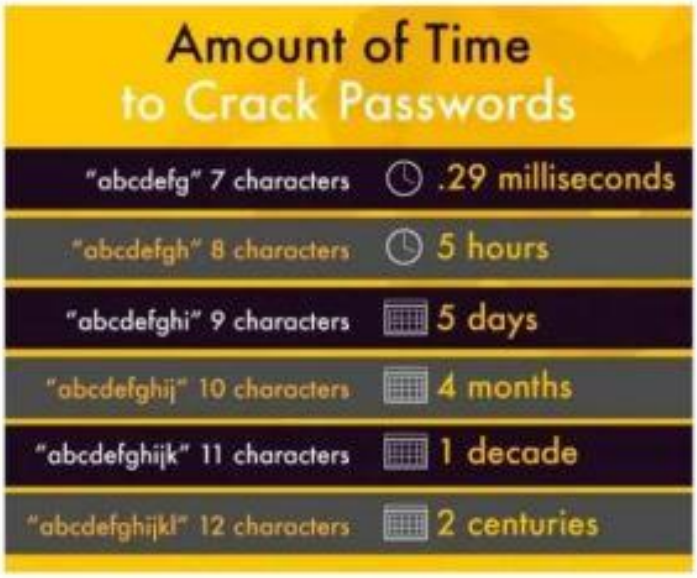
- **استفاده از ! به جای i یا @ به جای a** (فقط به یاد داشته باشید که این کار را به صورت تصادفی انجام دهید و بعنوان یک قانون کلی استفاده نکنید.)
- **استفاده یکی در میان از کلید شیفت؛** مثلا رمزی مانند behnam را میتوانید به شکلBeHnAm به کار برید.
- **تایپ کردن با قراردادن انگشتان در خانه های اشتباه:** در این روش کلمه یا جمله مورد نظر خود را انتخاب و آن را به خاطر بسپارید اما در هنگام تایپ، حروف ردیف بالایی یا پایینی را جایگزین کلمه یا جمله مورد نظر خود کنید. به عنوان مثال کلمه behnam با جایگزینی حروف ردیف بالایی همین کلمه تبدیل میشود به کلمه نامفهوم g۳hqj، البته همانطور که گفته شد سعی کنید در بین حروف از اعداد نامنظم مانند ۶،۸،۲،۵،۰ یا کاراکترهایی همچون @ ،&، *، $ هم استفاده کنید.
- یک روش دیگر انتخاب رمز عبور این است که کلمه یا جمله های فارسی را به عنوان رمز عبور در نظر گرفته، به جای حروف فارسی از **حروف انگلیسی ای که روی آن حروف فارسی قرار گرفته** است استفاده کنید. به عنوان مثال کلمه عبور «بهنام» در این روش " fikhm " میشود.

حال که با برخی شیوه ها و روشهای رمزگذاری آشنا شدید، بهتر است با مشخصات یک رمز عبور مناسب نیز آشنایی داشته باشید:

- **حتی الامکان دارای اطلاعات شخصی کاربر، مانند سال تولد، نام و ...نباشد.**
- **طول کلمه عبور حداقل بیش از ۸کاراکتر تشکیل شود.**
- **شامل کلمات رایج و موجود در فرهنگ لغت نباشد.**
- **ترکیبی از کاراکتر های متنوع، مانند حروف کوچک و بزرگ، اعداد، کاراکتر های خاص &، $، #، @، ^، %و ...باشد.**
- **یک رمز عبور ایجاد کنید که بتوانید به خاطر بسپارید، این کار از اینکه رمز عبورتان را در جایی بنویسید اجتناب می‌کند و این اصلا توصیه نمی‌شود.**
- **گذر واژه را هر دو هفته یکبار و یا زمانی که مشکوک هستید که کسی آن را می‌داند تغییر دهید.**
- **از رمز عبوری که قبلا استفاده کرده‌اید استفاده نکنید.**
- **از یک کلمه عبور برای سایت های مختلف استفاده نکنید چون در صورت لو رفتن یک کلمه عبور باقی اکانت های شما نیز به خطر خواهد افتاد.**

از نکات فوق اینگونه می توان دریافت که معمولاً قدرت یک رمز عبور به عنوان تابعی از میزان **پیچیدگی** یا **تصادفی** بودن کاراکترهای آن محسوب می شود، یعنی اینگونه تصور می شود که هر قدر از نمادها، اعداد و حروف بزرگ و کوچک بیشتری به صورت تصادفی استفاده کنید، ضریب امنیت پسورد بالاتر خواهد رفت ولی به یک نکته مهم دیگر هم باید توجه ویژه داشت که زمان هک شدن یک کلمه عبور رابطه نمایی (توانی) با تعداد کاراکترهای آن دارد، بنابراین

تنها مقدار کمی افزایش در طول پسورد می تواند مدت زمان مورد نیاز برای هک کردن را به شدت افزایش دهد. (با توجه به جدول شماره ۱)



جدول شماره ۱

روش تست میزان امنیت رمز عبور

پس از ساختن رمز عبور، می توانید میزان امنیت آن را مورد آزمایش قرار دهید و قدرت آن را بسنجید. برای انجام این کار، سامانه ها و سایت های بسیاری وجود دارند. به عنوان مثال، در گوگل عبارت "تست پسورد "را می توانید جستجو کنید www.passwordmeter.com . توجه داشته باشید که ممکن است نتایج سایت های مختلف متفاوت باشند. یعنی، امکان دارد یک پسورد در سایتی، ضعیف تشخیص داده شود ولی در سایت دیگر متوسط یا قوی اعلام گردد. خلاصه اینکه اگر طول پسورد را به **۸ کاراکتر یا بیشتر** برسانید و همینطور از کاراکترهای متنوع و خاص استفاده کنید، کلمه عبور شما قوی تر می شود. در نتیجه، حدس زدن آن توسط هکرها و سامانه های نفوذ به سختی قابل انجام خواهد بود. ضمن اینکه سعی کنید هر چند وقت کلمه عبور حساب خودتان را تعویض کرده و به خاطر بسپارید.

امنیت رایانه

نکات مهم برای حفظ امنیت رایانه شخصی

با وجود اینکه رایانه های شخصی باعث راحتی انجام برخی از فعالیت های روزمره شده اند، ولی همیشه در معرض خطر و تهدیدهایی از جمله ویروسها و بدافزارها، هکرها و حتی مفقود شدن اطلاعات شخصی هستند. بنابراین رعایت برخی نکات جهت حفظ امنیت رایانه های شخصی بسیار مهم است.

- **نکته اول :** استفاده از نرم افزارهای محافظتی **(مانند ضد ویروسها)** و به روز نگه داشتن آنها
- **نکته دوم :** باز نکردن نامه های دریافتی از منابع ناشناس
- **نکته سوم :** عدم ورود به سایتهای ناامن
- **نکته چهارم :** استفاده از گذر واژه های مناسب
- **نکته پنجم :** محافظت از کامپیوتر در برابر نفوذ با استفاده از حفاظت **فایروال (دیواره آتش)**
- **نکته ششم :** قطع اتصال به اینترنت در مواقع عدم استفاده
- **نکته هفتم :** تهیه پشتیبان از داده های مهم و حیاتی سیستم
- **نکته هشتم :** بررسی منظم امنیت کامپیوتر

حریم شخصی آنلاین

چرا حریم شخصی آنلاین مهم است و چگونه باید از داده هایمان محافظت کنیم ؟

- **نبود حریم شخصی آنلاین، کاربران را آسیب پذیر می کند .**

هنگامی که به اینترنت متصل می شویم و فعالیت های خود را آنلاین دنبال می کنیم از خودمان **ردپای دیجیتال** به جا می گذاریم. این رد پاهای دیجیتال مشخص می کنند که ما در چه ساعتی می خوابیم ، چه عادت هایی داریم ، وضعیت سلامتی ما چگونه است ، عادت های خرید ما چیستند و موارد بسیار زیاد دیگر . این داده ها می تواند در دسترس شرکت های تبلیغاتی زیادی با اهداف مختلفی قرار بگیرد . با توجه به رشد شبکه های اجتماعی و میل کاربران به فعالیت در این شبکه ها ، حجم زیادی از اطلاعات توسط خود کاربران در اینترنت توزیع می شود . یکی از رایج ترین روش های سوء استفاده از این اطلاعات ، ایجاد حساب جعلی است. هر چقدر بیشتر اطلاعاتتان را به اشتراک بگذارید ، همانقدر کنترل کمتری روی اطلاعاتتان دارید .

- **به خطر افتادن آزادی بیان**

حریم شخصی جزء اساسی آزادی بیان است . محافظت از حریم شخصی برخی گروه ها مانند فعالان حقوق بشر ، روزنامه نگاران، سیاستمداران برای جلوگیری از اذیت های احتمالی بسیار مهم است . هر چند حفظ حریم شخصی برای افرادی که در گروه های بالا نیستند هم بسیار مهم است .

- **حریم شخصی روی اعتبار ما تاثیر گذار است.**

بیشتر ما داستان هایی داریم که دوست داریم شخصی و خصوصی باقی بماند. ۵۰ سال پیش محافظت از همچین داستان هایی بسیار سخت و پیچیده نبود اما امروزه با توجه به تکنولوژی اینترنت و انواع سرویس های آنلاین و رد پاهای دیجیتالی که به جا می گذاریم ، حفظ اسرار سخت تر می شود .

- **از حریم شخصی خود محافظت کنید و امن بمانید .**

خیلی مشکل است که تمام رد پاهای آنلاین خود را پاک کنید ، اما راه هایی وجود دارند که کمک می کنند میزان اطلاعاتی که ناخواسته به اشتراک می گذاریم را به حداقل برسانیم .

فیشینگ

فیشینگ و راه های مقابله (حملات مهندسی اجتماعی و کلاهبرداری)

فیشینگ راهی است که تبهکاران، اطلاعاتی نظیر کلمه کاربری، رمز عبور، شماره ۱۶رقمی عابر بانک، رمز دوم و CVV۲ را از طریق ابزارهای الکترونیکی ارتباطات به سرقت می برند. شبکه های اجتماعی، سایت های حراجی و درگاه های پرداخت آنلاین نمونه ای از ابزار های الکترونیکی ارتباطات می باشند.

کلاهبرداری فیشینگ از طریق ایمیل ها و پیامها صورت می پذیرد و قربانیان به صورت مستقیم، اطلاعات حساس و محرمانه خود را در وب سایت های جعلی که در ظاهر کاملا شبیه وب سایت های سالم و قانونی می باشد وارد می نمایند. حقه فیشینگ یکی از تکنیک های مهندسی اجتماعی برای فریب کاربران می باشد که علی القاعده از ضعف امنیتی یک وب سایت برای انجام عملیات مجرمانه خود استفاده می کنند. برای اولین بار حقه فیشینگ در ۱۹۸۷ تعریف شد و اولین باری که واژه فیشینگ برای نام گذاری این واژه استفاده گردید، سال ۱۹۹۶بود.

انواع مختلف فیشینگ کدام است؟

فیشینگ انواع مختلفی دارد که به روش های مختلف تلاش میکنند به اطلاعات بانکی شما از طریق روش های متنوع مهندسی اجتماعی(Social Engineering) در حوزه فیشینگ مانند ایمیل، تماس تلفنی، صفحات جعلی پرداخت، پیامک، انواع مدل های ربات های تلگرام و انواع روش های جدیدی که انتظار آن نمی رود، دست یابد. برخی از معروفترین روشهای فیشینگ عبارت اند از:

فیشینگ با ایمیل های فریبنده

در این روش از حمله های فیشینگ، شخص کلاهبردار با ارسال ایمیل های فریبنده به قربانیانش میکوشد با بیان دلایل مجاب کننده مخاطبان را به وارد کردن اطلاعات بانکی خود وادار کند . ممکن است ایمیل به ظاهر از طرف بانک شما، یک شرکت معتبر یا حتی بانک مرکزی ارسال شود و از شما درخواست کند ظرف زمان معینی اطلاعات بانکی خود را ارسال کنید. متاسفانه بارها افرادی فریب این حملات فیشینگ را خورده اند.

نکته : سیستم مالی و بانکی هیچگاه از طریق ایمیل از شما درخواست نمیکند اطلاعات بانکی تان را برای آنها ارسال کنید، شما حتی مجاز به اعلام رمز بانکی خود به کارکنان بانک هم نیستید.

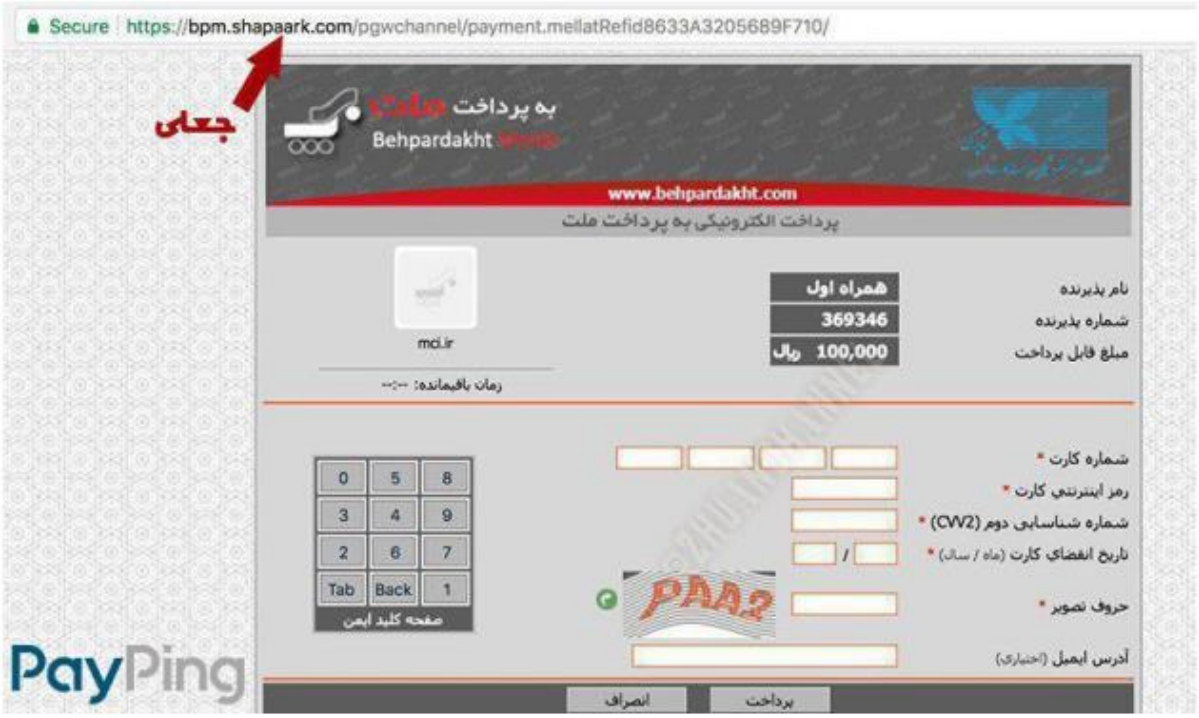
فیشینگ تلفنی

هکرها در این روش از طریق تلفن با طعمه های خود ارتباط برقرار میکنند و ضمن اینکه خود را نماینده بانک، شرکت معتبر و یا سازمانی که شما میشناسید معرفی میکنند، از شما می خواهند جهت دریافت جایزه خود اطلاعات بانکی خود را در اختیار ایشان قرار دهید. یا در روشی دیگر، با ارسال پیامک به شماره همراه شما، اعلام می کنند که حساب بانکی شما دچار مشکل شده است و شما را به زنگ زدن به شماره تماسی جعلی (سرویس تلفن اینترنتی) سوق می دهند و در ادامه از شما شماره حساب و رمز کارت و یا حتی رمز دوم را می خواهند.

نکته :برای واریز هر گونه وجه به حساب شما اعم از جایزه، پاداش و مزایا، نیازی به اعلام رمز بانکی شما نخواهد بود. برای مقابله با هکرها و حملات فیشینگ این نکته را فراموش نکنید.

طراحی صفحه ای نظیر درگاه پرداخت بانک

شخص هکر در این روش صفحه های مشابه درگاه پرداخت آنلاین بانکها طراحی میکند و با قرار دادن این صفحه جعلی در فروشگاه های صوری و با ارائه پیشنهاد های وسوسه کننده خرید سعی میکند شما را وادار کند وارد صفحه پرداخت جعلی که طراحی کرده بشوید و وجه انتقال دهید. به محض ورود به این صفحه جعلی و ارائه اطلاعات بانکی، اطلاعات شما به صورت خودکار برای هکر ارسال میشود و او قادر خواهد بود حساب شما را خالی کند. امن ترین درگاه پرداخت، درگاه پرداخت بانک مرکزی به آدرس **https://xxx.shaparak.ir** است و در کنار آن حتما باید نام یکی از **psp ها** (**شرکت های پرداخت الکترونیک**) مطرح درج شده باشد.



نکته : بهترین روش مقابله با این نوع از حمله های فیشینگ دقت به URL درگاه پرداخت است. درگاه های پرداخت بانک ها از کدهای امنیتی باضریب اطمینان بالا استفاده میکنند و اغلب در آدرس سایت عبارت **https://** قابل مشاهده خواهد بود.

فیشینگ با دستگاههای POS و ATM تقلبی

برخی کلاهبرداران با استفاده از POS و ATM تقلبی، کارت های بانکی طعمه های خود را کپی کرده و به بهانه فروش محصول و کالا، رمز عبور آنها را میپرسند و سپس به راحتی حساب بانکی افراد را خالی میکنند.

نکته: بهتر است هیچ گاه رمز عبور خود را در اختیار فروشندگان قرار ندهید. با پیشرفت تکنولوژی، شیوه های پرداخت متنوعی در اختیار شما قرار گرفته که با کمک آن میتوانید استفاده از POS و ATM را به میزان قابل توجهی کاهش دهید. دریافت دستگاه های POS اختصاصی توسط شرکتها و سازمانها هم میتواند به جلب اعتماد بیشتر مشتریان کمک کند.

ربات تلگرام و فیشینگ

ربات های تلگرام این روزها به بسیاری از کارهای ما سرعت بخشیده اند، شرکتهای معتبر هم در این خصوص خدمات خوبی را ارائه میدهند که گزارش گیری انتقال وجوه را ساده تر کرده است. اما به هر حال تلگرام بستر مناسبی برای انتقال وجه نیست و دیده شده به بهانه انتقال وجه و یا حتی دریافت خدمات و یا خرید محصولی و یا حتی با نوشتن پست های وسوسه برانگیز و تحریک افراد برای عضو شدن در کانال و یا گروه هایی، اطلاعات بانکی حساب و یا کارت بانکی شخص را سرقت می کردند.

روش های کاربردی در مقابله با فیشینگ

با توجه به مواردی که مطرح شد، راه هایی در مورد مقابله و جلوگیری از گیر افتادن در دام فیشر ها وجود دارد که از میان آنها می توان به موارد زیر اشاره داشت:

- **یکی از بهترین راه ها برای دستیابی به صفحات وب، نوشتن آدرس آن به طور مستقیم در مرورگر است.** یک ایمیل یا پیامک کلاهبرداری، این امکان را دارد که ادعای داشتن اعتبار لازم را داشته و از بانک، شرکت و یا مؤسسه معتبری ارسال شده باشد. هنگامی که شما روی لینکی که برای شما ارسال شده کلیک کنید با سایتی مشابه با سایت واقعی و به ظاهر معتبر مواجه میشوید که با پر کردن اطلاعات خود در آن، امکان به سرقت رفتن اطلاعاتتان را فراهم می کنید. برای جلوگیری از این اتفاق همیشه دنبال منابع معتبر بروید و در صورت دریافت ایمیلی با مقدمه های وسوسه بر انگیز، به جای بازگشایی، بلافاصله آدرس اصلی سایت مطرح شده را در مرورگر خود وارد کنید. همچنین سعی کنید امنیت اکانت ایمیل خود را افزایش دهید.
- **استفاده از رمز یکبار مصرف را جدی بگیرید؛** این رمز یکبار مصرف ها با اعتباری که در زمان کم دارند، باعث جلوگیری از به سرقت رفتن اطلاعات شما می شود.
- **فرستنده یا فرستاده غیر معمول؛** اگر پیامک یا ایمیلی از شخص ناشناسی دریافت کردید که دارای لینکی برای دریافت جایزه یا قرعه کشی بود و حتی اگر این پیام از طرف شخصی بود که او را می شناختید، به هیچ وجه بر روی آن لینک کلیک نکنید.
- **هدایت به دامنه فیشینگ به جای سایت واقعی؛** همانطور که در قسمت های بالا هم گفته شد، همیشه قبل از انجام تراکنش، آدرس **URL** درگاه پرداخت را حتما بررسی کنید.

امنیت اطلاعات

امنیت اطلاعات و ایمن سازی بانک های اطلاعاتی

امنیت اطلاعات و ایمن سازی شبکه های رایانه ای از جمله مسئولیت هایی است که مستلزم توجه همه کاربران صرف نظر از موقعیت شغلی آنها می باشد. برای بالا بردن امنیت در شبکه های رایانه ای و اطلاعاتی، آموزش و توجیه صحیح همه کاربران، وجود دستورالعمل های لازم برای پیشگیری از نقایص امنیتی، وجود سیاست های مشخص و مدون به منظور برخورد مناسب و به موقع با اشکالات امنیتی، از جمله مسائلی است که عدم توجه به آنها، عملکرد سازمان و افراد مرتبط با سازمان را تحت تاثیر قرار می دهد.

سه اصل کلیدی امنیت

در بحث امنیت اطلاعات، رعایت سه اصل مهم **حفظ محرمانگی، یکپارچگی و دسترس پذیری** می تواند مشکلات زیادی از این حوزه را برطرف نماید. اگر این سه اصل به درستی رعایت شود اطلاعاتی که درون بانکهای اطلاعاتی ذخیره میشوند قابل استناد بوده و این اطمینان خاطر وجود خواهد داشت که افراد غیرمجاز نمی توانند با دستکاری این اطلاعات، به سوءاستفاده از آنها بپردازند.

- **محرمانگی به معنای عدم دسترسی افراد غیرمجاز به اطلاعات است.** برای محرمانه نگه داشتن اطلاعات، داده ها رمزنگاری میشود و در طی انتقال یا جاهایی که ممکن است ذخیره شود (در پایگاه های داده، فایل های ثبت وقایع سامانه، پشتیبان گیری، چاپ رسید، و غیره) رمز شده باقی میمانند.

اشکال مختلف نقض محرمانگی : ضبط اطلاعات محرمانه نمایش داده شده روی صفحه نمایش رایانه، سرقت رایانه قابل حمل حاوی اطلاعات حساس و یا ارائه اطلاعات محرمانه از طریق تلفن. موارد ذکر شده از مهمترین موارد نقض محرمانگی است.

- **یکپارچگی به معنای جلوگیری از تغییر داده ها به طور غیرمجاز و یا تشخیص تغییر در صورت دستکاری غیرمجاز اطلاعات.** یکپارچگی وقتی نقض میشود که اطلاعات نه فقط در حین انتقال بلکه در حال استفاده یا ذخیره شدن به صورت غیرمجاز تغییر داده شود. سامانه های امنیت اطلاعات به طور معمول علاوه بر محرمانه بودن اطلاعات، یکپارچگی آن را نیز تضمین میکنند.

- **دسترس پذیری یعنی اطلاعات باید زمانی که مورد نیاز افراد مجاز هستند در دسترس باشند.** این بدان معنی است که باید از درست کار کردن و جلوگیری از اختلال در سامانه های ذخیره و پردازش اطلاعات و کانال های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد. سامانه ها باید در همه حال حتی در زمان قطع برق، خرابی سخت افزار و ارتقاء سامانه نیز در دسترس باقی بمانند. یکی از راه های از دسترس خارج کردن اطلاعات و سامانه اطلاعاتی، درخواستهای زیاد از طریق خدمات از سامانه اطلاعاتی مورد نظر می باشد، که در این حالت چون سامانه توانایی و ظرفیت چنین حجم انبوه خدمات دهی را ندارد از خدمات دادن به طور کامل یا جزئی عاجز میماند.

نتیجه گیری: امنیت در حوزه فناوری اطلاعات یک فرایند پیچیده **نرم افزاری و سخت افزاری** است. به طوری که سازمانها برای پیاده سازی درست زیرساخت های ارتباطی و بانکهای اطلاعاتی مجبور هستند بر مبنای خط مشی های دقیق و حساب شده ای از تجهیزات و ابزارهای امنیتی استفاده کنند تا داده های حساس سازمانی در امنیت بالا باشند و خدمات ارائه شده توسط سازمان با چالش روبرو نشوند .

امنیت ویندوز

امنیت در سیستم عامل ویندوز

حفظ امنیت در اینترنت و دنیای دیجیتال علاوه بر شباهت های آن با دنیای واقعی، تفاوتهای بزرگی نیز دارد. بنابراین ضروری است کلیه کاربران نسبت به سیستمها و سرویس هایی که با آنها در ارتباط هستند و خطرات محیط دیجیتال و راه های جلوگیری، آگاهی اولیه داشته باشند.

یکی از سیستم عامل های محبوب روی کامپیوترهای رومیزی و لپتاپ ها، ویندوز (Windows OS) میباشد . در ادامه موارد مرتبط با حفظ امنیت در سیستم عامل ویندوز را مورد بررسی قرار می دهیم.

۱- نصب نرم افزار آنتی ویروس: بعد از نصب سیستم عامل ویندوز، گام بعدی نصب یک نرم افزار آنتی ویروس به روز و مطمئن روی سیستم مورد استفاده می باشد.

۲- نصب نرم افزارهای ضد نرم افزار های مخرب: حتی بهترین آنتی ویروس ها هم ممکن است برخی نرم افزارهای مخرب را تشخیص ندهند. بنابراین علاوه بر نصب آنتی ویروس (که همیشه باید فعال باشد)، نصب یک نرم افزار برای تشخیص نرم افزارهای مخرب روی سیستم و فعال نمودن آن در بازه های زمانی مشخص برای اسکن کامل سیستم، ضروری است.

۳- فعال و تنظیم کردن Firewall یا دیواره آتش: برنامه Firewall هم مانند آنتی ویروس از کامپیوتر مورد استفاده محافظت میکند. در حالی که نرم افزارهای آنتی ویروس، برنامه ها و فایل های روی کامپیوتر را اسکن میکنند، برنامه دیواره آتش، ترافیک اینترنت بین کامپیوتر و بقیه شبکه (اینترنت) را کنترل میکند . برای حفظ امنیت در سیستم عامل ویندوز ، برنامه دیواره آتش را فعال نمایید. این برنامه را از طریق Control Panel فعال یا On کنید. در ویندوز ۱۰ از گزینه Advanced در پنجره به روز رسانی ویندوز استفاده و گزینه Automatic را انتخاب نمایید.

۴- به روز کردن : آپدیت یا به روز رسانی ویندوز باید در حالت خودکار قرار گیرد، در قسمت جستجوی برنامه ها در سیستم عامل ویندوز عبارت Windows Updateرا جستجو و از پنل سمت چپ پنجره باز شده، روی Change settings کلیک و مطمئن شوید Install updates automatically انتخاب شده است.

۵-حساب کاربری جداگانه : برای ورود به محیط ویندوز، داشتن دو حساب کاربری مهم است. یک حساب کاربری با دسترسی مدیریت (Administrator) برای نصب و حذف برنامه ها و دیگری برای کارهای روزانه.

۶-امنیت و به روز رسانی مرورگر : مرورگر هم مانند ویندوز و نرم افزارهای نصب شده باید به روز رسانی گردد. هر اکستنشن یا افزونه ای نباید روی مرورگر نصب شود و همچنین جاوا اسکریپت روی مرورگر فقط برای وبسایت های مورد اطمینان، فعال شود.

۷-رمزگذاری: اگر کامپیوتر به سرقت رفت یا شخصی توانست به کامپیوتر مورد نظر دسترسی پیدا کند، میتواند فایلها و اطلاعات شخصی و مهم را در اختیار بگیرد، بنابراین می توان با رمزگذاری فایل های مهم یا رمزگذاری سیستم عامل ویندوز، خطر دسترسی به اطلاعات مهم را کاهش داد.

۸-رمزعبور : کاربر برای ورود به هر حساب کاربری باید یک رمز عبور پیچیده و منحصر بفرد داشته باشید. بهترین روش استفاده از نرم افزارها یا ابزار **مدیریت رمزعبور** می باشد.

نکته پایانی :

یک سیستم عامل مثل یک مرکز فرماندهی به کاربر اجازه افزایش یا کاهش امنیت و سطوح دسترسی کامپیوتر را می دهد. سیستم عامل ویندوز به داشتن نقاط آسیب پذیر فراوان مشهور است، اما اگر کاربر قصد نصب سیستم عامل دیگری (مانند لینوکس) را نداشته باشد، تنظیمات امنیتی ویندوز تا زمانی که بر روی حالت **پیش فرض** هستند هیچ تاثیری در امنیت کامپیوتر مورد استفاده ندارد و باید به صورت **شخصی** فعال گردد، بنابراین داشتن آگاهی اولیه در مورد روش های بالا بردن امنیت کامپیوتر مورد استفاده و حفاظت از اطلاعات حیاتی و ضروری است.

فریب های اینترنتی

راهکارهای پیشگیری از فریب های اینترنتی

شیوع کرونا تاثیر بسیاری در زمینه رشد کسب وکارهای اینترنتی داشته و استقبال مردم به انجام امور و خریدهای اینترنتی نسبت به دوران قبل از شیوع این ویروس بسیار متفاوت است، اما پیش بینی میشود پس از پایان همه گیری کرونا و بازگشت مردم به زندگی عادی نیز رونق کسب وکارهای اینترنتی حفظ شود، زیرا خرید و انجام امور در بستر فضای مجازی و اینترنت در حال تبدیل به یک فرهنگ در جامعه امروزی است.
با توجه به شرایط کنونی جامعه، اکثر کسب وکارها به سوی فضای مجازی و سایتهای خرید و فروش آنلاین سوق یافته که در این بین کلاهبرداران سایبری با ترفندهای مختلف از کاربران اقدام به کلاهبرداری میکنند. بعضی اوقات مشاهده میشود که کاربران فضای مجازی و شهروندان برای تهیه لوازم مورد نیاز خود با مراجعه به سایتهای خرید و فروش، با سهل انگاری و زود اعتماد کردن، در دام مجرمان سایبری گرفتار میشوند.

۱- بدون شناخت و بی هدف عضو هر گروه یا کانال نشوید و هچنین روی هر لینکی کلیک نکنید: پیامک تسهیلات بانکی، وام مسکن، بسته رایگان اینترنت و...روش خوبی برای فریب می باشد، بنابراین بی جهت کلیک نکنید.

۲- توجه به عبارت https: در صورتی که به درگاه بانکی هدایت شدید، قبل از اینکه شماره کارت خود را وارد کنید، در قسمت آدرس بار از اعتبار دستگاه مطمئن شوید، یک درگاه مطمئن باید دارای عبارت **https** باشد.

۳- نمایش قفل: در کنار **https** در قسمت آدرس بار باید یک قفل وجود داشته باشد که علامت تایید کننده سرویس دهنده است.

۴- به استوری های سلبریتی ها شک کنید: عاقبت برخی از تبلیغات سلبریتی ها و میکروسلبریتی ها معمولا به صفحات تقلبی بانکی میرسد. این استوری ها معمولا با ویدیوهایی مثل «تخفیف های باورنکردنی و قیمتهای غیرقابل باور» فقط برای فریب دادن افراد طراحی شده اند.

۵- توجه به کد امنیتی: معمولا در صفحات فیشینگ، این کد امنیتی یک عکس ثابت است که با رفرش کردن صفحه تغییری نمیکند.

۶- یک بار اطلاعات غلط وارد کنید: یکی از اطلاعات کارت بانکیتان را اشتباه وارد کنید. اگر پیغام خطایی در صفحه کامپیوتر دریافت کردید یعنی به احتمال زیاد این صفحه جعلی نیست.

۷-چک کردن دامنه سایت: در سایت **enamad.ir** با کلیک و سرچ کردن صفحه بانکی که در آن قرار داریم به ما اعلام میشود که در حال استفاده از سایت جعلی هستیم یا نه.

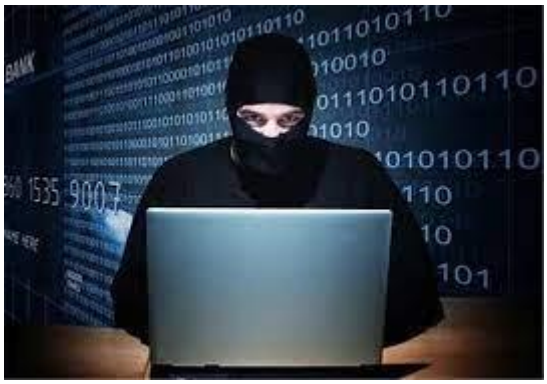
۸- افزونه ضد فیشینگ: یک افزونه یا اکستنشن ضد فیشینگ در سیستم خود نصب کنید که با وارد شدن در سایت مورد نظر به شما اعلام کند این صفحه از امنیت کافی برخوردار است یا نه.

۹- یک کارت بانکی برای خرید آنلاین داشته باشید: یک کارت خالی صرفا برای خرید کردن داشته باشید تا هنگام خرید به اندازه نیازتان ابتدا پول را به آن منتقل کنید.

۱۰-اگر تصمیم دارید تلفن همراه خود را بفروشید حتما تمام اطلاعات موجود در آن را پیش از فروش پاک کنید.

۱۱- سعی کنید دوستان و اعضای خانواده خود را از نکات امنیتی و کلاهبرداری های اینترنتی آگاه کنید، زیرا در اغلب موارد نداشتن اطلاعات کافی در این زمینه موجب بروز کلاهبرداری میشود.

۱۲- اجازه ندهید هر کسی به سیستم شخصی مورد استفاده فلش متصل نماید .



امنیت پیام رسان

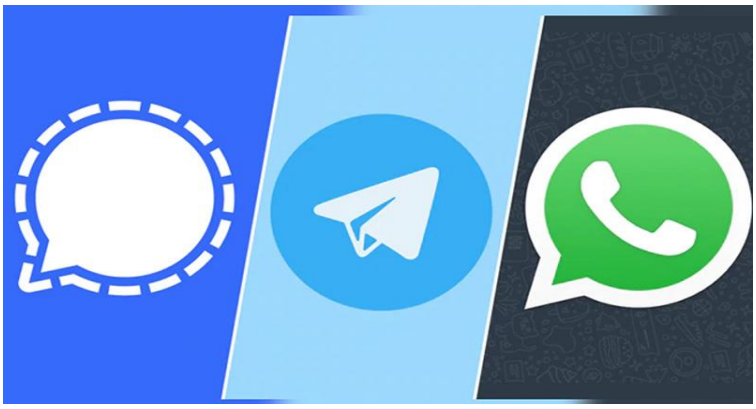
امنیت پیام رسان های ایرانی و خارجی

امروزه بحث داغی درباره امنیت پیام رسان های اینترنتی همه جا وجود دارد. مخصوصا این بحث با خبر فیلتر شدن تلگرام شدت بیشتری گرفته است. عده ای معتقدند که پیام رسان های خارجی مانند تلگرام و واتس اپ (که در ایران بیشتر شناخته شده هستند) از امنیت بسیار بالایی برخوردارند. عده ای هم به هیچ عنوان حاضر نیستند پیام رسان های داخلی (سروش، ایتا ...) را نصب کنند. اما به نظر شما امنیت کدام اپلیکیشن ها بالاتر است؟

منظور از امنیت پیام رسان چیست؟

امنیت پیام رسان به زبان ساده یعنی کسی از اطلاعاتی که شما در این شبکه ها به اشتراک میگذارید، با خبر نشود. این افراد میتوانند سازمان، شرکت، هکر، رسانه، نهاد های امنیتی و یا حتی دولت ها باشند. اطلاعات شما هم همه آن چیزی است که درون این برنامه ها وارد میکنید، مانند عکس، پیام، شماره تلفن، ایمیل، آدرس، نام کاربری، موقعیت مکانی(Location)، جنسیت و غیره.

هرچقد افراد کمتری بتوانند به این اطلاعات دسترسی داشته باشند، امنیت پیام رسان بالاتر میرود. به عبارتی، هر چقدر دست یابی به اطلاعات شما سخت تر و غیر ممکن تر باشد، برنامه ای که از آن استفاده میکنید امنیت بالاتری دارد .



چگونه دیگران میتوانند به اطلاعات ما دسترسی داشته باشند؟

وقتی که شما در یک سرویس پیام رسان عضو میشوید، حتما باید اطلاعاتی را وارد کنید. در این مرحله برای شما یک حساب کاربری ساخته میشود که از این به بعد معرف شما در دنیای آن پیام رسان خواهد بود. سپس شما میتوانید اطلاعات خود را در این شبکه ها به اشتراک بگذارید. بعضی از **سرویس های پیام رسان** (یا به طور کلی تر، **شبکه**

های اجتماعی) ممکن است اطلاعات خاص تری را از شما بگیرند. مثلا اینستاگرام بیشتر روی اشتراک گذاری فیلم و عکس تمرکز دارد یا در پیام رسان تلگرام شما میتوانید به راحتی با بقیه اعضای این پیام رسان، ارتباط داشته باشید و انواع مختلفی از فایل ها را رد و بدل کنید.

اما همه این عکس ها، پیام ها، ایمیل ها، شماره تلفن ها و اطلاعاتی که به این سرویس میدهید، در جایی ذخیره میشوند. به عنوان مثال اگر دقت کرده باشید، وقتی با گوشی های دیگری به غیر از موبایل شخصی تان، به اکانت تلگرام خودتان وارد شوید، همه چت ها، گروه ها و کانال هایی که روی موبایلتان بود را دوباره خواهید دید.

این مسئله به این معناست که اطلاعات شما در جایی به غیر از حافظه گوشی موبایلتان ذخیره شده اند. در حقیقت همه این موارد روی سرور های پیام رسانی که از آن استفاده میکنید ذخیره خواهند شد. در این سرور ها، اطلاعات روی جدول هایی ذخیره میشوند که از مجموعه این جداول کنار هم، **دیتابیس (پایگاه داده)** به وجود می آید.

خب! الان برای رسیدن به اطلاعات، فقط کافی است که کسی بتواند به دیتابیس های اصلی پیام رسان شما (که معمولا در محل شرکت پیام رسان قرار دارند) دسترسی پیدا کند. وظیفه شرکت پیام رسان این است که امنیت این داده ها را در برابر دیگران حفظ کند.

چگونه امنیت پیام رسان حفظ میشود؟

یک پیام رسان با تعریف کردن **الگو های رمز نگاری** ایمن میشود. یک پیام رسان ایمن، اطلاعاتی که شما به اشتراک میگذارید را رمز گذاری میکند. از این طریق کسی نمیتواند بفهمد که اصل داده ها چه چیزی بوده است. رمزنگاری هم کیفیت های متفاوتی دارد. الگو های رمزنگاری یک پیام رسان ایمن، باید پیشرفته و غیر قابل نفوذ باشند.

رفتارهای امن

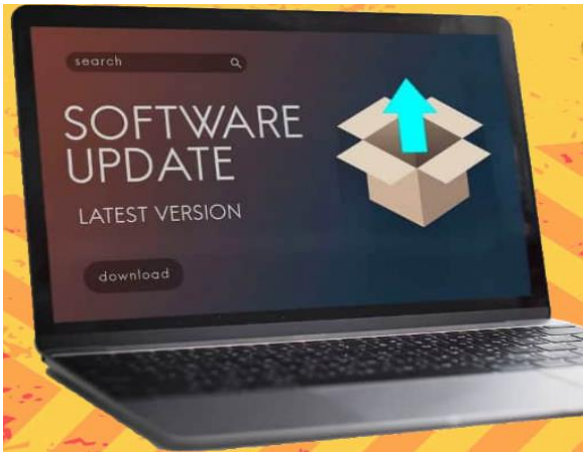
راهنمای رفتار امن در مواجهه با مسائل امنیتی و تهدیدات سایبری

این راهنما شامل توصیه‌ها و الزاماتی است که کارکنان باید برای امنیت اطلاعات در فعالیت‌های سایبری رعایت کنند:

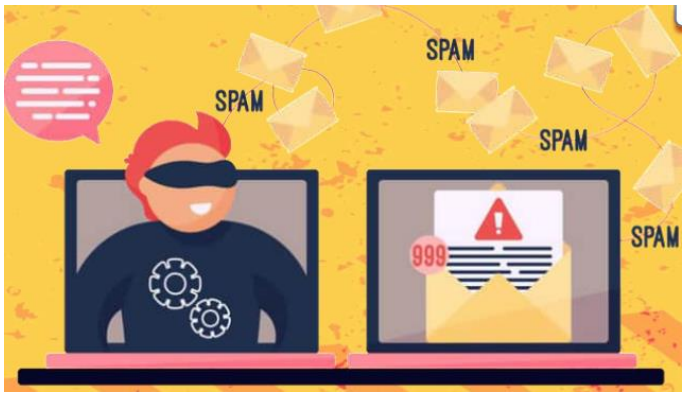
۱- **رمزنگاری:** توصیه می‌شود که از رمزنگاری برای حفاظت از اطلاعات حساس استفاده شود.
همیشه از اتصال امن به سامانه‌ها، (**پروتکل HTTPS**) استفاده نمایید. (مثلاً HTTPS://mis.ajums.ac.ir)

۲- **به‌روزرسانی نرم‌افزار:** الزام بروزرسانی نرم‌افزارها و سیستم‌عامل‌ها بطور مداوم.

رایانه خود را به سامانه مرکزی بروزرسانی‌های سیستم عامل ویندوز در مرکز داده دانشگاه متصل نمایید. (برای این مورد از کارشناس رایانه محل خدمت خود درخواست کمک کنید)



۳- **ایمیل‌های مشکوک:** ایمیل‌های مشکوک از آدرس‌های ناشناخته را باز نکنید و یا اطلاعات شخصی به آنها ارسال نکنید. اگر ایمیلی ناشناخته یا مشکوک دریافت کردید، آن را حذف کنید و به هیچ عنوان آدرس های موجود در آن باز ننمایید.

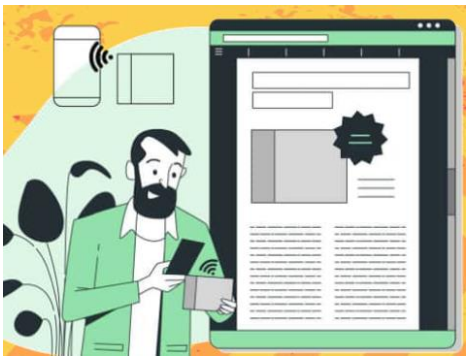


۴- **حفظ رمزها:** رمزهای خود را محرمانه نگه دارید و آنها را با دیگران به اشتراک نگذارید.

رمزهای سامانه‌های اتوماسیون اداری، مالی، آموزشی، اینترنت، بیمارستانی و..... را با همکاران خود به اشتراک نگذارید، زیرا مسئولیت هرگونه فعالیت توسط نام کاربری شما، مستقیماً بر عهده خود شما می‌باشد.

۵- **حفظ داده‌ها:** داده‌ها را با دقت حفظ کنید و به اشتباه با دیگران منتشر نکنید.

"حفظ اسناد و اطلاعات حساس در محل های ایمن و مطمئن و عدم به اشتراک گذاری اطلاعات حساس از قبیل نامه های اداری در شبکه های مجازی"



۶- **تلفن‌های همراه:** برای تلفن همراه رمز عبور مناسب در نظر بگیرید.

تلفن همراه خود را همیشه قفل کنید و از تأیید رمز دو مرحله ای برای ورود به برنامه های حساس (مثلاً نرم افزارهای بانکداری) استفاده نمایید.

۷- **گزارش تهدیدات:** تهدیدات و حوادث امنیتی را به واحد امنیت سایبری گزارش دهید.

هرگونه تهدید و یا موارد امنیتی اعم از مشاهده فایل‌های مشکوک در رایانه، دریافت ایمیل‌های مشکوک، دریافت پیام‌های مشکوک بواسطه فعالیت در اینترنت و.... را به گروه زیرساخت و امنیت در مدیریت آمار و فناوری اطلاعات با شماره داخلی ۱۰۰۱ و یا خط مستقیم ۳۳۱۱۱۰۰۱ گزارش نمایید.