هشدارهای امنیتی در خصوص حفاظت از داده های شخصی در فضای سایبر

- نرم افزاری را که قصد نصب کردن اش را نداشته اید، نصب نکنید. آنتی ویروس های تقلبی زیادی هستند که با با شگردهای مختلف و فریبنده تلاش می کنند شما را وادار به نصب یک بدافزار بر روی سیستم تان بکنند. تنها کاری که باید بکنید این است که آن را نصب نکنید.
- اگر در حال وب گردی هستید، در صورت برخورد با درخواست نصب کدک ویدوئوی جدید، آن را کلیک نکنید چون ممکن است موجب نصب نرم افزار جدید بر روی سیستم تان شود. ویدوئو های جعلی بسیاری هستند که با حقه تلاش می کنند در فضای وب قربانی را وادار به ارتقای نرم افزارش کنند اما در حقیقت با این کار قصد نصب بدافزار بر روی رایانه ی قربانی را دارند.گول این حقه را نخورید.
- نرم افزاری را از فایل های ضمیمه ای ایمیل دانلود و یا نصب نکنید. اگر فایلی را در ایمیل دریافت کرده اید اطمینان حاصل کنید که از دسته فایل های قابل اجرا مثل فایل exe. نباشد. فایل های جعلی که از سوی فرصت طلبان و سودجویان به ایمیل شما ارسال می‌گردند ممکن است موجب آسیب به سیستم رایانه‌ی‌تان شوند. خاطر جمع باشید که هیچ بانکی برای شما از طریق ایمیل، نرم افزار آنتی ویروس یا برنامه کاربردی یا غیره نمی فرستد. مراقب باشید در دام این گونه کلاه برداری ها نیافتید.
- از یک ویروس‌یاب استفاده کنید. از وب‌سایتهای غیر مطمئن یا email های مشکوک فایلی Download نکنید. حتی اگر یک ویروس‌یاب دارید خیلی مواظب باشید زیرا ممکن است با ویروس جدیدی مواجه شوید که نرم‌افزار ضدویروس شما نتواند آن را تشخیص دهد برای یک حفاظت خوب همیشه آنتی‌ویروس خود را up to date به روز نگه دارید.
- تنظیمات حفاظتی خود را ارزیابی کنید. بیشتر نرم‌افزارها از قبیل مرورگرها، برنامه‌های چک ایمیل و ... که در اینترنت استفاده می‌شوند همواره تسهیلاتی ارائه می‌دهند که به شما کمک می‌کند نیازهای امنیتی خود را مدیریت کنید. فعال کردن برخی قابلیت‌های این نرم‌افزارها باعث راحتی در استفاده از آنها می‌شوند ولی ممکن است آسیب پذیری کامپیوتر شما را افزایش دهند.
- چنانچه ایمیلی با این مضمون دریافت کردید " با شماره ی ۸۰۰ که مربوط به انجام امور بانکی است، تماس بگیرید" هرگز این کار را نکنید. در پشت کارت اعتباری تان شماره تلفنی قرار دارد که صورت وضعیت حساب شما را عیناً ارائه می دهد. به شماره تلفنی که درایمیل تان آمده زنگ نزنید، در عوض به دنبال شماره در

صورت وضعیت حساب تان بگردید.حمله ی جدیدی موسوم به Vishing طراحی شده است که با طرح درخواست از کاربران برای تماس با یک سیستم پاسخگوی جعلی خودکار، آنها را ترغیب می کند تا شماره حساب و سایر اطلاعات حساس شان را وارد کنند.

- زمانی که ضمیمه‌های یک نامه (Attachment) را باز می‌کنید و فایل‌هایی را از جانب خانواده و دوستان دانلود می‌کنید یا ایمیل‌های ناشناخته را می‌پذیرید، مراقب باشید.
- برای محفوظ نگهداشتن رایانه‌ی خود از دسترسی غیر مجاز، تنها به صرف چند ثانیه زمان نیاز دارید. هر زمان که خواستید میز کارتان را ترک کنید، حتماً قبل از آن از قفل بودن صفحه نمایش رایانه‌تان مطمئن شوید.
- یک screen-saver را که بعد از طی زمان از پیش تعیین شده موجب قفل صفحه نمایش رایانه می‌شود، بر روی صفحه‌ی نمایش نصب کنید. در این صورت ورود مجدد ، نیازمند وارد کردن کلمه‌ی عبورخواهد بود.
- اگر رایانه ی شما بیش از یک کاربر دارد، حساب‌های جداگانه‌ای با کلمه‌های عبور و login های منحصر به فرد برای هر یک ایجاد کنید.
- از کلمه ی عبور مطمئن استفاده کنید. یک کلمه ی عبور ایده آل و قابل اعتماد ترکیبی از حروف بزرگ و کوچک به اضافه‌ی اعداد و حداقل یک کارکتر خاص است. هرگز گزینه‌ای را که به رایانه امکان به خاطرسپاری کلمات عبور را می دهد فعال نکنید.(Hint)
- هرگز از یک کلمه ی عبور برای چند حساب یا دستگاه همراه استفاده نکنید.
- ابتدا از خود بپرسید، آیا لازم است این داده های حساس را انتقال دهم؟ اگر پاسخ تان به این سوال منفی بود، از کپی کردن اطلاعات تان بپرهیزید.
- دستگاه های قابل حمل را در جای مطمئن نگهدارید. اگر از آنها استفاده نمی کنید، آنها را دور از دسترس و در صورت امکان در کشوها و یا کابینت های قفل شده قرار دهید.
- یکی دیگر از مهمترین مواردی این که شما باید تا تمامی برنامه‌های امنیتی نظیر آنتی ویروس‌ها و فایروال‌ها و همچنین برنامه‌های کاربردی خود را همواره به روز نگه دارند در عین حال اقداماتی نظیر پاک نمودن کش مرورگر خود و همچنین داده های ذخیره شده مانند کلمه عبور می تواند ایده خوبی برای برقراری امنیت تبلت و گوشی های هوشمند باشد.این موارد باعث می‌شود که اگر در موقعیتی این وسایل در اختیار افراد غیر مجازی قرار گرفت نتوانند از مواردی چون حساب شما در وب‌سات ها و یا حساب ایمیل باز شما سو استفاده کنند و قانون پاک نگه داشتن باید برای لاگین های روزمره و برنامه های کاربردی سازمان اعمال گردد.

- داده های دستگاه قابل حمل خود را با گذرواژه ی مناسب رمزگذاری کنید.
- مطمئن شوید که از همه ی اطلاعات حساس و مهم دستگاه، بک آپ تهیه کرده اید.
- زمانی که به بلوتوث دستگاه نیاز ندارید آن را غیرفعال کنید.
- اطلاعات شناسایی مثل شماره سریال و اتیکت دستگاه را در صورت امکان ثبت کنید.
- در صورت به سرقت رفتن دستگاه، موضوع را هر چه سریعتر به مراجع ذی صلاح گزارش دهید.
- شبکه‌های بی سیم عمومی و رایانه‌های کیوسک گونه در مکان‌هایی مثل کافی نت‌ها، مراکز کنفرانس، هتل‌ها، مسافرخانه‌ها و فرودگاه‌ها همواره در معرض حمله‌ی خلافکاران و سودجویان قرار دارند. در صورتی که این شبکه‌ها و رایانه‌های عمومی آلوده شده باشند و شما بی خبر از این موضوع اقدام به تایپ گذرواژه‌ی خود نمایید، مهاجمین بلافاصله گذرواژه‌ی شما را به سرقت می برند. تغییر گذرواژه هر چند وقت یکبار و عدم استفاده از یک گذر واژه‌ی واحد برای چند رایانه یا سیستم می‌تواند بهترین راهکار برای مقابله با سرقت‌هایی از این دست در فضای سایبر باشد. به طور کل رایانه های عمومی قابل اعتماد نیستند، اما اگر چاره‌ای جز استفاده از آنها ندارید، گذر واژه‌ی خود را پیش از log off کردن یا در اولین فرصت تغییر دهید.
- یکی دیگر از مواردی که لازم است تا حتما در مورد آن صحبت گردد این است که به هیچ عنوان از اینترنت بی سیم غیر امن استفاده نکنید . بسیاری از افراد زمانی که متوجه می شوند که مکانی نظیر یک کافی شاپ دارای یک Hotspot Wi-Fi است سریع به آن متصل شده و شروع به وبگردی با اکانت‌های محرمانه خود می‌کنند که این کار بسیار اشتباه است چرا که افراد سود جو می توانند از طریق روش هایی به هنگامی که شما با خیال راحت در حال چک کردن اطلاعات محرمانه خود هستید شروع به جاسوسی در اطلاعات شما بکنند بدون اینکه شما از این موضوع با خبر شوید .
- به هیچ عنوان زمانی که در مکان های عمومی هستند از اینترنت‌های نا امن استفاده نکنند و تا زمانی که به یک شبکه خصوصی و یا VPN دسترسی نیافته اند به رد و بدل کردن اطلاعات محرمانه شرکت نپردازند.
- شبکه های خصوصی مجازی یا همان VPN های قانونی به کارکنان کمک می کند تا زمانی که دور از دفتر کار خود هستند بتوانند به راحتی و با اطمینان خاطر به تبادل اطلاعات بپردازند و به شکلی امن به اطلاعات درون کمپانی دست پیدا کنند بنابراین کمپانی‌ها می‌توانند یک شبکه مجازی راه اندازی کنند و از این تونل امن به تبادل اطلاعات حتی از راه دور بپردازند و زمانی که کارکنان به این شبکه متصل شدند بتوانند به راحتی به تبادل تصاویر و فیلم و سایر فایل های مهم خود بپردازند.
- از خود رفتارهای نامناسبی مثل قلدری، مزاحمت ، گستاخی و مجرمانه در فضای سایبر نشان ندهیم.

- از کلمه ی عبور یا هر نوع اطلاعات هویتی که متعلق به ما نیست استفاده نکنیم.
- کلاهبردارهای فیشینگ از پست الکترونیک جعلی و وب‌سایت‌های تقلبی، با ظاهری بسیار شبیه شرکت‌های تجاری قانونی استفاده می‌کنند، تا کاربران ناآگاه را برای افشای اطلاعات لاگین یا حساب کاربری شخصی فریب دهند. برای اطمینان، اگر ایمیلی از یک شرکت تجاری یا بانک دریافت داشتید که شامل لینکی به یک وب‌سایت است، اطمینان یابید که وب‌سایتی که شما از آن بازدید می‌کنید، قانونی و قابل اطمینان باشد.
- به ایمیل‌های ارسالی با عنوان" کنترل پهنای باند اینترنت" که به ظاهر از سوی سرویس‌های تامین کننده اینترنت ارسال می‌شود توجه نکنید.

اگرچه متأسفانه هیچ راه قطعی برای پیشگیری از حمله‌ی منع سرویس توزیع شده وجود ندارد، اما با اتخاذ تمهیدات زیر می‌توان از احتمال اینکه مهاجمین رایانه‌ی شما را برای حمله به سایر رایانه‌ها انتخاب کنند، کاست:

- یک نرم افزار آنتی ویروس بر روی سیستم خود نصب و نگهداری کنید.
- Firewall را بر وی سیستم تان نصب و آن را به گونه ای پیکربندی کنید تا تعداد ترافیک ورودی و خروجی از سیستم محدود شود.
- تدابیر امنیتی مناسب را برای توزیع ایمیل تان به کار ببندید. اعمال فیلترهای ایمیل می تواند تا حدی به شما در مدیریت ترافیک ناخواسته کمک کند.

- وقتی از کامپیوتر خود استفاده نمی‌کنید، اتصال خود با اینترنت را قطع کنید. کسانیکه از تکنولوژی DSL یا ADSL یا اینترنت سرعت بالا استفاده می‌کنند، معمولاً مدت زیادی کامپیوتر خود را در این وضعیت قرار می‌دهند، که ریسک بالایی دارد. چون خرابکاران و ویروس‌ها دائماً شبکه‌ها و اینترنت را برای شناسایی کامپیوتر قربانی اسکن می‌کنند و حال اگر کامپیوتر شما مدام به اینترنت متصل باشد احتمال نفوذ به آن بسیار بیشتر است.
- گاهی پیش می آید زمانی که با همکار خود در مورد مسائل کاری در حال گفتگو هستید، متوجه نیستید که شاید کسی در اطراف‌تان در حال شنود مکالمه‌ی شما باشد. از این رو به شما توصیه می‌کنیم که در صورتی که مکالمه‌ی محرمانه ی دارید تا زمانی که از امن بودن محیط اطراف تان مطمئن نشده اید، طرف مقابل تان را پشت خط نگه دارید. در ضمن به خاطر داشته باشید که هرگز اطلات خصوصی و محرمانه ی خود را با افراد غریبه در میان نگذارید.