امنیت کاربران در دنیای مجازی

شرکت حلماگستر خاورمیانه

واحد پشتیبانی فنی

فهرست مطالب :

فصل اول: آموزش بالا بردن امنیت اینترنت وایرلس (WiFi) و شبکه های بی سیم

فصل دوم: ایجاد یک رمز عبور قوی

فصل سوم: چگونه قدرت دفاع و محافظت از رایانه خود را در مقابل نرم افزارهای مخرب افزایش دهیم؟

فصل چهارم: کنترل حجم مصرفی اینترنت

فصل پنجم: امن کردن فضای سایبر برای کودکان

فصل ششم: پرداخت الکترونیک امن

فصل هفتم: مسدود کردن پورت های غیرضروری

فصل اول: آموزش بالا بردن امنیت اینترنت وایرلس (WiFi) و شبکه های بی سیم

بسیاری از کاربران در خانه و محل کار از اینترنت بی سیم استفاده می کنند، به این دلیل که ارتباط با آن آسان و بدون محدودیت است. اما ممکن است این آسانی و بدون محدودیت بودن کار دست کاربران دهد و باعث هک شدن و یا ایجاد اختلال شود. آیا می دانید برای بالا بردن امنیت و کارآیی شبکه وایرلس خود چه اقداماتی باید انجام دهید؟

نگرانی‌های امنیتی

تنظیمات پیش فرض بیشتر مودم‌های خانگی امنیت کمی را تامین می کنند. مودم‌های خانگی:

- از طریق اینترنت مستقیماً در دسترس اند
- به راحتی قابل شناسایی اند
- معمولاً در تمام زمان‌ها روشن اند
- و در بسیاری از حالت‌ها به خاطر بد تنظیم شدن آسیب پذیر اند.

موارد فوق به مهاجم امکان حمله را می‌دهد. در کنار این موارد، ویژگی بی سیمی که روی بسیاری از این دستگاه‌ها هست، آسیب پذیری‌های دیگری را اضافه می‌کند.

مقابله و پیشگیری از تهدیدات امنیتی

مراحل مقابله با حملات روی مودم‌های خانگی، برای افزایش امنیت مودم‌های خانگی و کاهش آسیب پذیری شبکه داخلی در برابر حملات منابع خارجی است. برخی از این مراحل عبارتند از:

۱- نام کاربری و رمز عبور ورود به تنظیمات مودم خود را تغییر دهید

سازندگان برای دسترسی کاربر به صفحه تنظیمات دستگاه، نام کاربری و کلمه عبور پیش فرضی را روی این دستگاه‌ها تنظیم می‌کنند. این کلمات عبور و نام کاربری‌های پیش فرض به راحتی در دسترس عموم هستند و برای مهاجمان هم شناخته شده‌اند؛ بنابراین باید سریعاً در هنگام نصب اولیه مودم تغییر کنند. یک کلمه عبور قوی می‌تواند ترکیبی از حروف و اعداد با ۱۴ کاراکتر یا بیشتر باشد. بعلاوه، توصیه می‌شود کلمه عبور را هر ۳۰ تا ۹۰ روز تغییر دهید.

معمول ترین username و Password ها admin و admin میباشند

۲- **WPS را خاموش کنید**

این سرویس اجازه می دهد تا کاربران با وارد کردن سریال ۸ رقمی درج شده روی Access Point به آن وصل شوند. با غیرفعال کردن آن کاربران تنها با دانستن رمزعبور می توانند، وصل شوند.
امروزه نرم افزارهای هک وایرلس که قابلیت نصب بر روی کامپیوتر و یا دستگاه های موبایل را دارند به سادگی در دسترس کاربران عادی و حرفه ای قرار گرفته است و با توجه به نقص در تکنولوژی wps مشکلاتی را از قبیل هک مودم و استفاده از اینترنت کاربران بوجود آورده است. جهت جلوگیری از هک شدن مودم پیشنهاد میگردد wps را در مودم خود به صورت نرم افزاری خاموش نمایید و هیچگاه دکمه wps را بر روی مودم فشار ندهید .

۳- **استفاده از رمزنگاری برای محرمانگی داده‌ها:**

تکنولوژی بی سیم تلاش می کند پیغام را به گونه ای ارسال کند که به وسیله سایر دستگاه ها قابل خواندن نباشد. امروزه چنین تکنولوژی برای کپسوله سازی وجود دارد. طبیعتا شما خواستار انتخاب بهترین شکل از رمزنگاری اطلاعات هستید که بتوانید شبکه خود را امن کنید. پس برای این کار همه ی ابزار های (wireless) شبکه باید از رمزنگاری شناخته شده ای استفاده کنند.
الگوریتم WEP با هدف فراهم کردن محرمانگی داده (احراز هویت و رمزنگاری) توسعه یافت اما نقاط ضعف بسیاری دارد. این الگوریتم توسط استاندارد 802.11 – که به عنوان دسترسی محافظت شده Wi-Fi (WPA) پیاده سازی می‌شود، جایگزین شد. در حال حاضر WPA2، نسخه جدیدتر WPA است. WPA و WPA2 با استفاده از تغییر پویای کلیدها، احراز هویت و رمزنگاری قویتری را فراهم می‌کنند. WPA و WPA2 در دو نسخه سازمانی و شخصی موجود هستند.
WPAشخصی (WPA-PSK) برای خانه‌ها و ادارات کوچک که از کلیدهای از قبل به اشتراک گذاشته شده و بدون نیاز به سرور احراز هویت استفاده می‌کنند، توسعه یافتند. اگر از WPA–PSK استفاده می‌کنید، از کلید از قبل به اشتراک گذاشته شده بلند، استفاده کنید و آن را در فواصل معینی تغییر دهید.
WPA سازمانی نیازمند سرور احراز هویت RADIUS است، از پروتکل احراز هویت قابل توسعه (EAP) استفاده می‌کند، و امنیت بیشتری را فراهم می‌کند اما نیازمند بودجه بیشتر و پیاده سازی پیچیده‌تر است.
WPA2 از رمزنگاری ۱۲۸ بیتی AES استفاده می‌کند. WPA2 با استفاده از رمزنگاری AES امنیت را بیشتر تامین می‌کند و تمام دستگاه‌های بیسیم باید با WPA2 سازگار باشند. اگر استفاده از WPA2 امکان پذیر نیست، WPA گزینه جایگزین است. WEP کمترین امنیت را فراهم می‌کند. در صورت استفاده از WEP، باید از گزینه کلید ۱۲۸ بیتی آنهم با طولانی‌ترین کلید از قبل به اشتراک گذاشته شده که مدیر مودم می‌تواند آنرا مدیریت کند استفاده شود.

۴- **SSID پیش فرض را تغییر دهید**

شناسه مجموعه خدمات (SSID) نام یکتایی برای شناسایی شبکه محلی بیسیم (WLAN) است. تمام دستگاه‌های بیسیم برای برقراری ارتباط با یکدیگر باید از SSID یکسانی استفاده کنند. سازندگان عموماً SSID پیش فرضی را برای این دستگاه‌ها تنظیم می‌کنند که بیانگر نام سازنده یا خود دستگاه است. مهاجم می‌تواند از این نام پیش فرض برای شناسایی دستگاه و هرگونه آسیب پذیری مرتبط با آن استفاده کند. کاربران گاهی اوقات SSID را نامی قرار می‌دهند که بیانگر سازمان، مکان و نام خود آنها است. این کار منجر به شناسایی راحتتر کسب و کار و یا نام شخص، برای مهاجم می‌شود. به طور مثال، SSID که نام شرکتی را منتشر می‌کند جذابتر از مودمی است که نامی مانند "ABC123" دارد. هنگام انتخاب SSID، از بهترین تجارب کاری خط مشی‌های پیچیدگی کلمه عبور استفاده کنید:

- ✓ تعداد کاراکترهای SSID باید بیشتر از ۸ کاراکتر باشد.
- ✓ از حروف و علامت‌ها (symbol) در SSID استفاده کنید.
- ✓ SSID را گاهاً تغییر دهید و از کلمات عبور قبلی استفاده نکنید.

۵- پخش عمومی SSID را خاموش کنید

در شبکه های بی سیم، نقطه دستیابی یا مودم به طور معمول نام شبکه (SSID) را تا فاصله ای مشخص پخش می کند. این خاصیت برای مشترکانی که در حال حرکت بین خارج و داخل این محدوده هستند، طراحی شده است. در منزل به این ویژگی نیازی نیست و این ویژگی، تعداد افرادی که دوست دارند به شبکه شما وارد شوند را افزایش می دهد. خوشبختانه بسیاری از wireless ها اجازه غیرفعال کردن ویژگی پخش عمومیSSID را به مدیر شبکه می دهد. که با غیر فعال کردن Broadcast ssid قابل انجام است.

۶- از فیلتر Mac Address استفاده کنید

هر قطعه از اجزایWireless ، دارای یک شناسه منحصر به فرد است که آدرس فیزیکی یا Mac Address نام دارد. نقاط دستیابی و مسیریابی، Mac Address تمام دستگاه هایی که به آن وصل هستند را در خود دارد. توسط این ویژگی می توان MAC Address دستگاه هایی که می خواهیم به شبکه وصل شوند را وارد مودم کنیم و فقط این دستگاه ها توانایی برقراری ارتباط را دارند. فقط توجه داشته باشید این ویژگی آنقدر که به نظر می رسد قدرتمند نیست و هکر ها به راحتی می توانند Mac Address ها را جعل کنند.

۷- اتصال خودکار شبکه های Wi-Fi را باز نکنید

اتصال به شبکه بی سیم باز، مانند شبکه بی سیم رایگان یا مودم همسایه شما، کامپیوترتان را در معرض خطر امنیتی قرار می دهد. هر چند به طور معمول فعال نیست ولی بسیاری از کامپیوتر ها تنظیماتی در دسترس دارند که اجازه می دهد این اتصال بدون اطلاع کاربر اتفاق بیفتد.

۸- به ابزار ها Static IP اختصاص دهید

بیشتر شبکه های خانگی تمایل به داشتن IP Address های پویا دارند. تکنولوژی DHCP براستی، برای تنظیم کردن راحت است اما متاسفانه این مزیت، ابزاری برای دزدان شبکه می باشد. کسانی که می توانند به راحتی IP Addressمجاز را از لیست DHCP شبکه شما بدست آورند. برای حفظ امنیت بیشتر از IP های ثابت استفاده کنید.

۹- از Firewall استفاده کنید

مودم های مدرن دارای Firewall های داخلی هستند اما گزینه هایی برای غیر فعال کردن آنها نیز موجود است. مطمئن شوید که Firewall مودم شما روشن است. دیوار آتش از ورود غیر مجاز جلوگیری می کند و در صورت صحیح بودن کلیه تنظیمات، می تواند بسیاری از درخواست های آلوده را شناسایی کند.

۱۰- مودم یا نقطه دستیابی را در مکانی امن قرار دهید (محدود کردن پوشش WLAN):

سیگنال های Wireless معمولا به خارج از خانه می رسند. نشت میزان کمی از سیگنال ها به بیرون مشکلی ندارد اما دسترسی بیشتر به این سیگنال ها کار را برای ردیابی و بهره برداری دیگران آسان می کند. موقعیت مودم، نقطه دسترسی تعیین کننده ی این دسترسی می باشد. در ساده ترین حالت، دستگاه مرکز یک دایره می باشد و داده ها را توسط امواج به صورت دایره ای شکل ارسال می کند. پس بهتر است مودم در قسمت های مرکزی خانه قرار دهیم.

LAN ها ذاتاً ایمن‌تر از WLAN ها هستند چراکه توسط ساختار فیزیکی که در آن هستند محافظت می‌شوند. پوشش WLAN اغلب فراتر از محیط خانه یا سازمان شما است. این امر شنود نفوذگرانی را که خارج از محدوده شبکه شما هستند امکان پذیر می‌کند. بنابراین، مکان قرار دادن آنتن، نوع آنتن و سطح قدرت انتقال جنبه‌های مهمی هستند که باید در نظر گرفته شود. محدوده پوشش را موقع امن کردن WLAN می‌توان محدود کرد. یک آنتن تمام جهته که در مرکز قرار گرفته است بیشترین نوعی است که استفاده می‌شود. در صورت امکان، از یک آنتن جهت دار برای هدایت پوشش WLAN به مناطق مورد نیاز استفاده کنید. آزمایش سطوح انتقال و قدرت سیگنال هم، پوشش شبکه را به مناطق مورد نیاز محدود خواهد کرد.

۱۱- شبکه را در دوره ی طولانی بی استفاده، خاموش کنید

اقدام نهایی برای امنیت Wireless ها، خاموش کردن دستگاه در مدت زمانی (طولانی) است که از آن استفاده نمی کنید. برای مثال اگر قصد سفر دارید، بهتر است دستگاه را خاموش کنید تا از نفوذ هکرها جلوگیری نمایید.
توجه داشته باشید که امنیت در شبکه یکی از مهمترین بحث های امنیت در کامپیوتر می باشد و باید سعی کنید که نکات امنیتی را رعات کنید تا دچار مشکلات امنیتی نشوید.
متاسفانه، تنظیمات پیش فرض بیشتر مودم‌های خانگی امنیت کمی را تامین می‌کند و شبکه‌های خانگی را نسبت به حملات آسیب پذیر می‌کند. کسب و کارها و سازمان‌های کوچک که بودجه‌ای برای زیرساخت‌های فناوری اطلاعات و پشتیبانی از کارمندان خود تخصیص نداده‌اند اغلب از همین مودم‌های خانگی برای اتصال به اینترنت استفاده می‌کنند. اینگونه سازمان‌ها هم اغلب از این مودم‌ها، بدون پیاده سازی اقدامات احتیاطی امنیتی استفاده می‌کنند.

۱۲- مودم خود را به روز رسانی کنید

در نظر داشته باشید که بسیاری از مشکلات نرم افزاری که خود باعث کاهش امنیت مودم و شبکه شما می گردد با تلاش برنامه نویسان برطرف می گردد.
پس لازم است Firmware مودم خود را جهت همسو کردن با این تغییرات نرم افزاری بر روز نگه دارید.

چگونه بدانیم که آیا کسی از وای فای ما استفاده می کند یا خیر؟
شاید برای شما هم این سوال پیش آمده باشد که چگونه بدانیم که آیا کسی از اینترنت وای فای ما استفاده می کند یا نه؟

کاربران اینترنت وای فای روز به روز به تعدادشان افزوده می شود، از استفاده عمومی (خانه) گرفته تا کارهای تجاری، بانک ها و ... از این رو اگر شما یک رمز عبور قوی برای خود انتخاب نکنید خطر بیرون همیشه در کمین خواهد بود.

خوشبختانه چندین تکنیک برای شناسایی استفاده غیر مجاز و هک مودم وجود دارد:

۱- راحت ترین و ساده ترین روش نگاه کردن به چراغ Router می باشد، به طور مثال شما کامپیوتر خود را در حالت Hibernate گذاشته اید و هیچ گونه ارتباط اینترنتی ندارید، با یک نگاه به Router می بینید که چراغ Internet دارد چشمک می زند، این یکی از نشانه های دزد می باشد، حالا خیلی از شماها الان

در این فکر هستید که این راه زیاد موثر نیست، بله درست فکر می کنید، حالا وقتی خودتان دارید با اینترنت کار می کنید آن وقت چگونه تشخیص داد که کسی از ما دزدی می‌کند یا نه.

۲- روش بهتر این است که به Router خود وصل بشید و از داخل پنل تنظیمات مودم خود و ورود به تنظیمات DHCP Clients ، به راحتی می توانید ببینید که آیا کسی به وای فای شما وصل است یا نه، این آدرس در برخیRouter ها کمی تفاوت دارد اما پیدا کردن آن زیاد سخت نیست، راهنمای وارد شدن در زیر هر Routerدرج شده است اما تقریباً تمامیRouter ها برای وارد شدن به تنظیمات از چنین روشی استفاده می کنند:

۱- Browser یی مثل Firefox باز کنید و آدرس 192.168.1.1 را وارد کنید.

۲- یوزر و پسورد به طور پیش فرض admin می باشد.

اگر بعد از انجام این کارها متوجه شدید که کسی دارد از شما دزدی می کند باید به دنبال راه حلی برای این مشکل باشید، یکی از راه حل‌ها همانطور که در بالا بیان شد گذاشتن پسورد قوی می باشد، توجه داشته باشید که از پسوردهایی مثل: تاریخ تولد، شماره موبایل و شماره شناسنامه و .... اکیداً خوداری کنید، سعی کنید پسورد ترکیبی داشته باشید. میتوانید جهت قرار دادن رمز قوی برای وایرلس خود به فصل دوم مراجعه فرمایید.

۳- میتوانید از نرم افزار who is on my wifi استفاده نمایید با نصب این نرم افزار روی دسکتاپ خود این نرم افزار با یک موتور ردیابی از طریق scan شبکه وایرلس شما به صورت دقیقه ای نشان می دهد که آیا افراد غریبه روی شبکه وایر لس شما نفوذ دارند یا خیر. این کار نیز می تواند تا حدودی شما را از وجود افراد غریبه با خبر کند .

فصل دوم: ایجاد یک رمز عبور قوی

شما چطور یک رمز عبور درست می کنید که در عین قوی بودن، یادآوری اش هم آسان باشد؟ این چالشی است که همه ما با آن روبرو هستیم،

گام اول یک رمز قوی درست کنید: Anatomy یک رمز قوی را در تصویر بالا می بینید، اما اگر بخواهیم موارد را تک تک توضیح دهیم، عبارت هستند از :

حروف بزرگ انگلیسی: استفاده از حروف انگلیسی در حالت بزرگ، بیش از آنچه تصورش را بکنید زمان لازم برای شکستن یک رمز عبور را افزایش می دهد .

Spacebar: امروزه بسیاری از سایت ها به شما امکان استفاده از Space Bar در رمزهای عبور را می دهند. اگر می توانید، از آن استفاده کنید، و در غیر این صورت از خط تیره (-) برای جدا کردن کلمات بهره بگیرید .

اعداد: در جاهایی که استفاده از اعداد منطقی است، آنها را به کار بگیرید، چون اگر یک ترتیب درست را در نظر نگیرید، به یاد آوردن آنها در استفاده های بعدی مشکل خواهد بود .

حروف کوچک انگلیسی: در نوشتار انگلیسی وقتی یک اسم یا نام کشوری را می نویسیم، حرف اول باید بزرگ باشد ولی حرف های بعدی کوچک. از اثر گذاری همین ترفند کوچک بر قوت رمز عبورتان، غافلگیر خواهید شد .

علایم: بهترین جا برای استفاده از علایم، انتهای رمزها است. بنابراین در صورت استفاده از آنها حتما سعی کنید یک علامت مهجور که کمتر کسی به آن توجه می کند را انتخاب کنید .

طول رمز: قوی بودن رمز، بیشتر با طولانی بودن آن در ارتباط است، نه با پیچیده بودنش! به جای یک رمز ۸ تا ۱۰ حرفی که از کلمات بی معنی تشکیل شده، از رمزی طولانی متشکل از چند کلمه، با ساختاری که در بالا توضیح داده شد استفاده کنید.

گام دوم از چند رمز استفاده کنید: با فرض رعایت تمام نکات بالا، اگر یک رمز را برای تمام حساب های خود به کار ببرید، معنای اش این است که هر چقدر هم آن رمز قوی باشد، ولی با شکسته شدنش تمام هویت آنلاین شما به خطر خواهد افتاد و نه فقط آن، بلکه با شکستنش، رمز حساب های بانکی تان هم به دست سارقان می افتد .

سعی کنید هرگز یک رمز را برای حساب های مختلف به کار نبرید و اگر در مهاجرت از یک رمز به رمز دیگر دچار مشکل می شوید، لااقل از این حقه موثر استفاده کنید: یک رمز برای شبکه های اجتماعی، یک رمز برای حساب های بانکی، و یک رمز برای ایمیل. به این شکل با از دست رفتن یکی از رمزها، به یک باره با مشکلات متعدد در هر سه حوزه روبرو نمی شوید.

گام سوم رمز واحد را برای هر حساب شخصی سازی کنید: تصور کنید که ساختار کلی رمز شما برای حضور در شبکه های اجتماعی این باشد My 1st Password!: اما برای اینکه امنیت خودتان را بالا ببرید، یک حقه کوچک بزنید و آن این باشد که به انتهای همین رمز برای حساب gmail خود، gml را اضافه کنید. یا به انتهای رمز Yahoo کلمه Yah، را و به انتهای رمز Reddit ، Redd را. در این صورت باز هم در عین رعایت سادگی، رمز های خود را تقویت کرده اید.

فصل سوم: چگونه قدرت دفاع و محافظت از رایانه خود را در مقابل نرم افزارهای مخرب افزایش دهیم؟

برای کمک به امن بودن رایانه خود در مقابل نرم افزارهای مخرب، دو رویکرد زیر را به شما پیشنهاد می دهیم :

۱ - باید قدرت دفاع رایانه خود را به روش های زیر افزایش دهید. چگونه؟

- ✓ از یک منبع معتبر برنامه های آنتی ویروس و ضد جاسوسی را تهیه و نصب کنید.
- ✓ هرگز برنامه هایی را که هشدار می دهد اگر نرم افزار را دانلود نکنید امنیت کامپیوتر شما به خطر می افتد یا خود را برای پاک کردن ویروس رایانه به شما پیشنهاد می دهد دانلود نکنید.
- ✓ برنامه های ضد نرم افزارهای مخرب را از مکان هایی که به آنها اعتماد دارید دریافت کنید.
- ✓ از پیشنهادات امنیتی مایکروسافت در مقابله با اینگونه نرم افزارها که بصورت رایگان است استفاده کنید. یا از لیست همکاران مایکروسافت که نرم افزارهای ضد برنامه های مخرب تولید می کنند یکی را انتخاب کنید.
- ✓ نرم افزار خود را به طور مرتب به روز کنید.
- ✓ مجرمان سایبری بی وقفه در تلاشند تا از ضعف نرم افزارها بهره برداری کنند، و بسیاری از شرکت های نرم افزاری برای مقابله با این تهدیدات بدون خستگی در تکاپو هستند. شما باید :

* همواره نرم افزارها، آنتی ویروس ها و برنامه های ضد جاسوسی، مرورگرها، سیستم عامل خود و... را به روز رسانی کنید.

* هرگاه نرم افزار شما پیشنهاد کرد بصورت خودکار به روز رسانی شود، آن را به روز رسانی کنید.(اغلب برنامه های اصلی این قابلیت را دارند)

* نرم افزارهایی را که از آنها استفاده نمی کنید حذف (Uninstall)کنید، این کار بسادگی از طریق Control Panel امکان پذیر است.

* از کلمه عبورهایی قدرتمند استفاده کنید که مخفیانه بمانند.

*کلمه عبورهای قوی حداقل دارای ۱۴ آرایه و ترکیبی از اعداد، حروف و نشانه ها باشد .

*کلمه عبور خود را فاش نکنید.

* از یک کلمه عبور برای همه سایت ها استفاده نکنید، اگر این کلمه به سرقت برود تمام اطلاعات شما در خطر است.

*اگر در منزل یا محل کارتان از ارتباط بی سیم استفاده می کنید از رمزهای عبور قدرتمند متفاوتی برای رمز روتر و دستگاه تان استفاده کنید.

* هیچگاه دیواره آتشین(Firewall) خود را غیر فعال نکنید.

* دیواره آتشین در واقع یک سد محافظتی میان رایانه شما و اینترنت برقرار می کند. حتی یک لحظه غیر فعال کردن آن می تواند ریسک حمله توسط نرم افزار های مخرب را افزایش دهد.

✓ از فلش ها با احتیاط استفاده کنید. وبرای کاستن از احتمال حمله اینگونه نرم افزار ها:

*از فلش های ناشناس بر روی رایانه شخصی خود استفاده نکنید

* هنگامی که فلش را به رایانه متصل می کنید دکمه Shift را نگه دارید. اگر اینکار را فراموش کردید، بر روی دکمه X که در سمت راست بالای صفحه هستند کلیک کنید تا صفحه بسته شود.

* اگر از داخل محتویات پوشه ها مطمئن نیستید، پوشه را باز نکنید.

۲ – از دانلود نرم افزار های گول زننده مخرب خودداری کنیم و به توصیه های زیر عمل کنید:

هنگامی که می خواهید یک ضمیمه را باز کنید یا برروی پیوند موجود در ایمیلتان یا صفحه شخصی خود در شبکه های اجتماعی، کلیک کنید، بسیار هوشیار باشید، حتی اگر فرستنده آن را می شناسید. ابتدا از دوستی که آن را برایتان ارسال کرده سوال کنید، اگر او برایتان ارسال نکرده بود صفحه را ببندید.

از کلیک کردن بروی کلمات OK ، I Accept و Agree در بنرهای تبلیغاتی خودداری نمایید.

تنها از سایت هایی دانلود کنید که به آنها اطمینان دارید .

در مواجهه با بازی ها، موسیقی ها و ویدئوهای رایگان که در برخی از سایتها وجود دارد نهایت هوشیاری را به خرج دهید. زیرا برنامه های مخرب معمولا از این موارد بعنوان طعمه برای خود استفاده می کنند و باعث بدنامی آنها شده اند.

فصل چهارم: کنترل حجم مصرفی اینترنت

نوع استفاده از اینترنت

میزان حجم مصرفی شما ارتباط مستقیم دارد با نوع استفاده شما از اینترنت

۱. مصرف عادی

شامل : مرور سایت ها و خواندن وبلاگ ها و وبسایت ها

۲. استفاده برای شبکه های اجتماعی

شامل: شبکه های اجتماعی اشتراک عکس، فیلم و ...

توجه داشته باشید سایت فیسبوک قابلیت نمایش اتوماتیک ویدئوهای به اشتراک گذاری دیگر کاربران را به صورت اتوماتیک دارد که از پهنای باند اینترنت شما استفاده میشود.

۳. استفاده از سایت های دانلود و برنامه هایی که فایل های حجیم در آن ها انتقال داده میشود.

۱. دانلود نرم افزار، ویدئو، کتاب و ...

۲. استفاده و دانلود برنامه های موبایل

۳. شبکه های اجتماعی موبایل (Telegram، tango یا whatsappp)

توجه داشته باشید تمامی فیلم ها و عکس های به اشتراک گذاری شده در گروه های وایبر بر روی گوشی شما دانلود شده و از پهنای باند اینترنت شما استفاده مینماید.

۴. آپدیت برنامه های موبایل (آپدیت اندروید، آپدیت بازی ها ،آپدیت برنامه ها)

۰۴ استفاده برای مشاهده دوربین مداربسته

کاربران میتوانند برای مشاهده دوربین های مداربسته از طریق ip استاتیک با استفاده از سرویس Adsl اقدام نمایند، به دلیل انتقال تصاویر حجم زیادی از پهنای باند را مصرف مینماید.

۰۵ استفاده چند کاربر از سرویس اینترنت

زمانیکه چند کاربر (مانند کافی نت) از اینترنت استفاده میکنند حجم مصرف شده برابر است با مجموع حجم هایی که هر کاربر از اینترنت استفاده نموده است. و طبیعی است زمانیکه چند کاربر از اینترنت استفاده مینمایند حجم مصرفی بالاتری نسبت به مشترکی که تنها با یک سیستم به اینترنت وصل میشود.

مواردی که باعث استفاده ناخواسته از اینترنت میشود

۱. آپدیت

✓ آپدیت ویندوز

- اولین مصرف کننده حجم مصرفی بدون اطلاع مشترک ویندوز می باشد
- ویندوز بنا بر تنظیمات اولیه خود هر روز یا هر هفته یکبار بدنبال بروزرسانی خود است.
- البته این بروز رسانی ها گاهی اوقات لازم است.

- شما می توانید تنظیمات را به گونه ای تغییر دهید که متوجه این بروزرسانی ها بشوید و یا اینکه کلا این بروزرسانی ها را جهت کاهش حجم مصرفی خود غیرفعال نمایید.

✓ آپدیت آنتی ویروس

- یکی از پرمصرف ترین برنامه های اینترنتی آنتی ویروس ها هستند که با روشن گذاشتن بروزرسانی خودکار آنها حجم قابل توجهی از سرویس شما کسر می شود.

✓ آپدیت برنامه های نصب شده بر روی ویندوز

- مانند برنامه آفیس و محصولات ADOBE :
- پیشنهاد می کنیم به محض نصب برنامه آفیس و محصولات ADOBE مثل Adobe acrobat reader بلافاصله تنظیمات بروز رسانی خودکار را در قسمت تنظیمات آنها غیرفعال کنید

۲. ویروس ها و تروجان ها

ویروس ها و تروجان ها ممکن است مشغول ارسال اطلاعات شما از طریق اینترنت برای صاحبان خود باشند و این جاسوسی حجم زیادی را از سرویس شما کسر می کند

۳. استفاده از فیلترشکن یا VPN

اکثر فیلترشکن های رایگان ابزارهای جاسوسی هستند که اقدام به نصب نرم افزارهای تبلیغاتی و مخرب بر روی ویندوز میکنند و برخی از داده های کاربر را بر روی سرور خودشان ذخیره میکنند که باعث کم شدن حجم مصرفی کاربر میشوند.

VPN ها نیز شبکه های مجازی خصوصی هستند که برای ارسال و دریافت داده ها، اطلاعات را رمزنگاری مینمایند که این امر باعث انتقال حجم بیشتری میشود.

۴. هک شدن مودم و رمز وایرلس

گاهی به دلیل ضعف امنیت و رعایت نکردن نکات ایمنی در تنظیم شبکه برخی از افراد اقدام به نفوذ به سیستم و استفاده از اینترنت شما مینمایند.

چک کردن امنیت مودم

گاهی دیگران بدون اجازه و با استفاده از ضعف تنظیمات مودم ، اقدام به استفاده از اینترنت و پهنای باند می نمایند. برای جلوگیری از دسترسی افراد غیر مجاز به اینترنت و پهنای باند خط شما میتوانید اقدامات زیر را انجام دهید:

۱. قراردادن پسورد از نوع wpa personal یا wpa2/psk
۲. قرار دادن رمز پیچیده برای وایرلس (رمز عبور ترکیبی از حروف، اعداد و علائم خاص باشد)
۳. عوض کردن رمز وایرلس به صورت دوره ای (هر شش ماه)
۴. ست کردن ip برای یوزرهای آشنا و بستن بقیه ip ها از طریق تنظیمات مودم (lock کردن ip ها)
۵. روشن کردن Firewall مودم

راه های تست حجم مصرفی

چنانچه از مقدار حجم مصرف شده سیستم خود اطمینان ندارید و یا نیاز دارید که اطلاع داشته باشید هر سیستم به تفکیک به چه میزان ترافیک مصرف نموده است می توانید از روش های ذیل کمک بگیرید

الف) روش های نرم افزاری

۱- نرم افزار BWmeter برای ویندوز:

از امکانات این برنامه می توان به موارد زیر اشاره کرد:

- ✓ نمایش گرافیکی و عددی مقدار پهنای باند مصرفی
- ✓ توانایی زیرنظر گرفتن و کنترل کردن پهنای باند مصرفی در شبکه ها
- ✓ توانایی محدود کردن دسترسی کاربران به برخی از سایت ها و سرعت های بالا
- ✓ تهیه گزارش روزانه هفته ای ماهانه و سالانه از مقدار پهنای باند مصرفی
- ✓ نمایش ترافیک های مشکوک و استفاده هکرها و ویروس ها و ...
- ✓ قابل اجرا بر روی تمامی نسخه های ویندوز

۲- نرم افزار Traffic monitor برای اندروید :

- ✓ از ویژگی های این نرم افزار می توان به موارد زیر اشاره کرد:
- ✓ کنترل و شمارشگر میزان آپلود و دانلود از طریق Wireless و Mobile access
- ✓ کنترل و نمایش ترافیک مصرفی توسط هر برنامه
- ✓ نمایش آمار ترافیکی روز و ماه گذشته
- ✓ اندازه گیری سرعت
- ✓ لغو اجرای برنامه های پر مصرف

۳- تنظیم مودم به حالت Bridge و اتصال از طریق کانکشن Broadband

در این حالت با تغییر تنظیمات مودم از حالت pppoe به حالت Bridge و ایجاد کانکشن Broadband با هر بار اتصال این کانکشن می توانید مقدار حجم مصرفی خود را که توسط این کانکشن محاسبه می گردد را بدست آورید

نکته در این نوع اتصال این است که در این حالت تنها فقط یک سیستم امکان اتصال به اینترنت را خواهد داشت.

ب) روش های سخت افزاری

میتوانید مودم خود را به یک دیوایس میکروتیک متصل نمایید تا قابلیت مانیتورینگ و کنترل مصرف کاربران متصل به شبکه را داشته باشید. و برای هرکاربر محدودیت زمانی و حجمی مجزا در نظر بگیرید. شما حتی میتوانید سایت های قابل بازدید توسط کاربر را نیز محدود نمایید.

فصل پنجم: امن کردن فضای سایبر برای کودکان

بخش اول: اینترنت و سلامت روانی کودکان

برای کاهش میزان آسیب پذیری کودکان و نوجوانان در فضای مجازی، توجه به نکات ذیل الذکر توسط والدین، می‌تواند کارساز باشد. اگر چه همواره مشاوره با پزشک و روانشناس، به خصوص روانشناسان سایبر، توصیه می‌شود.

۱. فهرستی از سایت‌های خوب و ارزشمند را در کنار مانیتور نصب کنید

سایت خوب، برای بچه‌های خوب حتماً نیاز هست. میلیون‌ها سایت وب، مناسب کودکان نیست. آن ها را جلوی صفحه جست وجوی گوگل قرار ندهید. مطلوب کودکان و نوجوانان نیست. سایت‌های خوب را شناسایی و به آن ها معرفی کنید تا همواره با این پرتال‌ها سرگرم باشند.

۲. از فرزند خود بخواهید که صفحات وب بوک مارک شده شما را بعضاً چک کند

وقتی شما صفحات وب را بوک مارک کنید، کودکان علاقمند می‌شوند از آن صفحات استفاده کنند که قبلاً ثبت شده بر روی مروگر. با بوک مارک کردن صفحات خوب، کودکان و نوجوانان را به استفاده از این پرتال‌ها ترغیب کنید.

۳. نکات مربوط به انتخاب صحیح کد کاربری و رمز عبور را به فرزندتان یادآوری کنید

اگر آن ها وارد صفحات شبکه‌های مجازی و پست الکترونیک می‌شوند، طریقه استفاده صحیح از آن پرتال‌ها و همچنین ثبت کد کاربری و رمز عبور دقیق و ایمن را، در نظر داشته باشید. همه چیز را باید به کودکان آموزش دهید.

۴. از ایشان بخواهید، رمز عبور خود را جایی یادداشت نکند

از کودکان و نوجوانان بخواهید که رمز عبور خود را جایی یادداشت نکنند. این موضوع بین این قشر سنی، زیاد مشاهده می‌شود.

۵. به فرزندتان آموزش دهید که هیچ صفحه ناشناسی را کلیک نکند

عدم کلیک کردن بر روی پاپ آپ ها و صفحات تبلیغی ناشناس، موضوعی است که باید به آن توجه کنید. این موضوع رابه فرزندانتان یاد بدهید و آموزش بدهید.

۶. به فرزندان خود یاد بدهید که مشاهده پرتال‌های مستهجن، چه عواقب منفی در پی دارد.

اینکه فکر کنید عدم صحبت کردن درباره سایت‌های مستهجن، کمکی به کودکان و نوجوانان شما است، اشتباه می‌کنید. آن ها را باید با عواقب استفاده از این پرتال‌ها آشنا کنید .سبک زندگی دیجیتالی را باید به کودکان خود مانند دست شویی رفتن و مسواک زدن و لباس پوشیدن، یاد بدهید. خیلی از مهارت‌های اجتماعی را کودکان و نوجوانان می‌توانند در محیط واقعی، از دیگران یاد بگیرند به طور مستقیم یا غیر مستقیم.

بخش دوم: کارهایی که والدین نباید انجام دهند

حضور افراد دارای فرزند در شبکه‌های اجتماعی از دو جنبه خود والدین و فرزندان قابل بررسی است که اشاره به چند نکته برای دور ماندن از آسیب‌های احتمالی خالی از لطف نیست.

علاوه بر فراگیری رسانه‌های اجتماعی بین گروه‌های مختلف سنی جامعه، در موارد بسیاری نیز دیده می‌شود که والدین به نیابت از فرزندان خود، حضور آنها را در رسانه‌های اجتماعی رقم می‌زنند..

۱. پروفایل خود را عمومی نکنید

هر کسی حق دارد حریم خصوصی اش را نسبت به سطح استفاده اش از شبکه های اجتماعی تنظیم کند. حریم خصوصی باید طوری تنظیم شود که فقط افرادی که با آنها در ارتباط هستید بتوانند پست هایتان را ببینند. همچنان می توانید حریم خصوصی هر پست را هم جداگانه تنظیم کنید و مراقبت بیشتری نسبت به اینگونه مسائل با فرزندان خود داشته باشید.

۲. عکس کودک دیگران را به اشتراک نگذارید

یکی از بزرگترین مشکلات این است که والدین عکسهای گروهی فرزندان را در شبکه های اجتماعی قرار می دهند. والدین حق دارند که بدانند چه کسانی این عکسها را می بینند و زیر آن نظر می گذرانند .اگر هم بخواهند می توانند این عکسها را دور از شبکه های اجتماعی نگه دارند.

۳. برای کودکان پروفایل نسازید

زمانی که کودکان به سن معقولی رسیدند دلایل زیادی وجود خواهد داشت تا در یک سایت‌های بزرگ و جهانی برای خود پروفایل بسازند.
گذشته از همه مسائل امنیتی، کودکان می توانند در آینده تصمیم بگیرند که داده هایشان را برای گردابهای تبلیغاتی باز بگذارند یا از این داده ها حفاظت کنند

بخش سوم: نرم‌افزارهای فیلترینگ خانگی برای مراقبت از فرزندانتان در فضای‌مجازی

آشنایی با خطرات و تهدیدات دنیای مجازی
بچه ها در هر سنی در معرض خطرند. نوجوانان مستقل و کارکشته اند و کمتر به هشدارهای بزرگ تر ها گوش می دهند. نوجوانان فکر می کنند که بهتر از بزرگ تر ها می دانند و بسیار تحت تأثیر همسن و سال ها و کنجکاوی ذاتی شان هستند .نوجوانان نیاز دارند به گونه ای متفاوت رفتار کنند. تحقیقات نشان می دهد عوامل زیر روی آن ها تأثیر می گذارد:

۱. سوء استفاده جنسی
۲. دیدن تصاویر خشن و مستهجن
۳. تهدید شدن توسط مسیج ها یا ایمیل
۴. فریب و گول خوردن
۵. معتاد شدن به اینترنت
۶. شست و شوی مغزی توسط وب سایت های تبلیغاتی و نفرت انگیز
۷. شکستن قوانین بدون این که کودکان متوجه این موضوع باشند .

راهکار نرم افزاری نظارت والدین
در پاسخ به این پدر و مادرهای نگران باید گفت خوشبختانه دنیای نرم افزار خود پاسخ نسبتا مناسبی به این معضل داده است و اگر به هیچ وجه امکان ندارد که فرزندانتان را از درگیر شدن با اینترنت منع کنید؛ می‌توانید با استفاده از نرم افزارهای فیلترینگ خانگی هم دسترسی آن‌ها را به سایت‌های نامناسب محدود کرده و هم از میزان و نوع استفاده آن‌ها از اینترنت آگاه شوید.
در واقع باید گفت همانطور که کودکان در دنیای واقعی نیاز به کنترل و مراقبت دارند، در فضای مجازی نیز باید مراقب آن‌ها بود. بخش زیادی از وقت کودکان در خانه و اوقات فراغت نوجوانان با ابزار و تکنولوژی‌های جدید و گوشی‌های هوشمند سپری می‌شود. باید خانواده‌ها نظارت دقیقی بر فعالیت کودکان و نوجوانان در فضای مجازی داشته باشند.

فضای مجازی، علیرغم همه مزایایش چالش‌های جدی بسیاری را نیز خصوصاً برای کودکان و نوجوانان ایجاد کرده است. کودکان در حالی که در جهان گسترده آنلاین مشارکت می‌کنند چیزهایی را که به این جهان ارسال شده مشاهده می‌کنند، وارد اتاق‌های گپ و گفت اینترنتی می‌شوند و یا به عضویت شبکه‌های اجتماعی در می‌آیند در معرض عناصر اجتماعی که در جهان واقعی از آن‌ها اجتناب می‌شود؛ نیز قرار می‌گیرند.
در حقیقت فضای مجازی یک فضای پالایش شده و استاندارد برای کودکان نیست و استفاده غیراصولی کودک از این فضا می‌تواند وی را در معرض آسیب‌های جبران‌ناپذیر مختلف قرار دهد. بهترین موارد استفاده از اینترنت برای کودکان زمانی است که یکی از والدین، آن‌ها را همراهی کند ویا اینکه موارد حفاظتی مانند فیلترینگ خانگی قبل از استفاده کودک از اینترنت لحاظ شده باشد.

اما فیلترینگ خانگی چیست؟ بهترین نرم افزارهای آن کدامند؟
این نرم افزارها می‌توانند به چند شکل مختلف اعم از محدود سازی دسترسی یا گزارش به والدین نظارت بر مصرف فرزندان را اعمال کنند. برخی از این نرم افزارها مخصوص اندروید یا گوشی هوشمند و تبلت و برخی نیز مخصوص ویندوز یا لپ تاپ ورایانه طراحی شده‌اند.

برخی از قابلیتهای نرم افزارهای کنترل و نظارت بر استفاده از کامپیوتر و اینترنت

- ✓ محدود کردن نرم افزار ها یا بازی هایی که کودکان اجازه استفاده از آنها را دارند
- ✓ جلوگیری از دسترسی کودک به فایل ها و پوشه های خاص
- ✓ ایجاد فیلترینگ برای سایت های غیر مجاز (دارای لیست سیاه از هزاران سایت غیراخلاقی)
- ✓ تنظیم سایت های محدودی که کودک اجازه استفاده از آنها را دارد
- ✓ ایجاد گزارش از میزان و نحوه استفاده کودک از کامپیوتر و کارهایی که انجام داده است
- ✓ ایجاد محدودیت روزانه برای ساعات استفاده از کامپیوتر
- ✓ تنظیم زمان قطع شدن اینترنت و خاموش شدن کامپیوتر
- ✓ تنظیم زمان مجاز استفاده از یک سایت خاص (مثلا سایت بازی آنلاین)
- ✓ نمایش تمام فعالیت هایی که کودک انجام داده است (به والدین)
- ✓ امکان ارسال گزارشات به ایمیل والدین
- ✓ محیط کاربری اسان بدون نیاز به آموزش خاص
- ✓ امکان استفاده در کامپیوترهای چندکاربره و عمومی (مثل مدارس و ادارات)
- ✓ تنظیم بازه زمانی مجاز برای استفاده از یک نرم افزار یا بازی (مثلا بازی Angry Bird فقط در ساعت ۶ تا ۸ شب)
- ✓ جلوگیری از دسترسی به تنظیمات ویندوز

✓ امکان کنترل نرم افزار از راه دور

در زیر نمونه هایی از این نرم افزارها معرفی می گردند که والدین محترم می توانند بر حسب نیاز خود و با توجه به قابلیتهای آنها نرم افزارر مورد نظر خود را یافته و مورد استفاده قرار دهند.

کیدلاگر(kidlogger)

این محصول این امکان را به افراد می‌دهد تا با نصب برنامه، مدیریت رایانه، موبایل، نوت بوک و... را در اختیار گرفت و گزارشات آنلاین همراه را با جزئیات در مورد ردیابی زمانی ایجاد داد. با استفاده از این نرم افزار می‌توان فهمید کاربر (فرزند و یا پرسنل تحت نظر) چقدر با کامپیوتر کار می‌کنند، لیست برنامه‌های استفاده شده، بیشترین مخاطبین مورد استفاده در تلفن همراه، رد یابی زمانی و محیط کاری، مانیتورینگ آنلاین، نظارت موبایل و کامپیوتر از راه دور و... را کنترل نمود.

آی نت (I net)

نرم افزار دیگر «I net» می‌باشد که امکانات کنترل فرزندان از راه دور را داراست. با استفاده از این نرم افزار می‌توان از تمامی فعالیت‌های فرزندان در هنگام استفاده از رایانه و اینترنت مطلع شد و حتی میزان دسترسی را برای فرزندان مشخص کرد و این دسترسی‌ها را محدود نمود.

پاساد(PASAD)

ضرورت بکارگیری این محصول؛ در فراهم آوردن امکان کنترل دسترسی فرزندان به اینترنت توسط والدین آنهاست. با این محصول براحتی می‌توانید نسبت به اوقات مجاز و غیرمجاز برای دسترسی به اینترنت فرزندان خود برنامه ریزی نمایید .همچنین این محصول از حیث نوع سایت‌ها و دسترسی به سایتهای غیراخلاقی امکانات کنترلی متنوع و سهل الوصولی را در اختیار شما می‌گذارد.

چایلدکنترل (Childcontrol)

نرم افزار «Salfeld Child Control» راهکارهای مناسبی برای کنترل والدین بر روش استفاده کودکان از کامپیوتر ارائه می‌دهد.

توسط این نرم افزار می‌توانید محدودیت‌های مورد نظر خود را ایجاد کنید تا با خیال راحت اجازه استفاده کودکان از کامپیوتر را بدهید.

این نرم افزار می‌تواند دسترسی به فولدرها، فایل‌ها، نرم افزارها، بازی‌ها، و... را محدود کند. یا فقط در ساعت‌های خاصی اجازه کار با کامپیوتر را بدهد. همچنین توسط این نرم افزار می‌توانید دسترسی به اینترنت را محدود کنید یا بعضی از سایت‌ها را فیل‌تر کنید. و یا فقط اجاره دسترسی به چند سایت خاص را بدهید.

جایگاه کودکان(Kids Place)

این اپلیکیشن بیشتر زمانی به کار خواهد آمد که قصد دارید دیوایس خود را برای مدتی در اختیار کودکان بگذارید. برای ورود به این برنامه و همچنین هنگام خارج شدن از آن باید رمز ۴ رقمی را که از پیش تعیین کرده‌اید را وارد کنید.

با استفاده از این برنامه می‌توانید تماس، ارسال پیام، یا نصب و پاک کردن برنامه‌های جدید را غیر فعال کنید، همچنین می‌توانید تماس‌های دریافتی را هنگامی که این برنامه در حال اجراست، غیر فعال کنید و اینترنت و سیگنال‌های بی‌سیم را نیز قطع کنید. (قابل استفاده علیه بچه‌های فامیل)!

قفل کننده اپلیکیشن(AppLock)

این برنامه یکی از محبوب‌ترین برنامه‌های این دسته است و در کنار پشتیبانی از ۲۴ زبان مختلف، ۳۰ میلیون کاربر نیز دارد.

از امکانات آن می‌توان قفل کردن پیام کوتاه، دفتر تلفن، برنامه‌ها مختلف، و همچنین کنترل بر روی عکس‌ها و فیلم‌های داخل گالری و پنهان کردن آن‌ها. با استفاده از این برنامه می‌توانید قسمت تنظیمات دیوایس خود را نیز قفل کرده و نگرانی از بابت تغییر آن‌ها نداشته باشید.

زمان دیده شدن(Screen Time)

این برنامه کمی با برنامه‌های دیگر متفاوت است و بیشتر مخصوص والدینی است که فرزندان بزرگ‌تر و نوجوان دارند.

میزان کنترل و دخالت والدین در این برنامه به نسبت کمتر است و امکانات آن محدود به مانیتور کردن و تعیین محدودیت استفاده از دیوایس و برنامه‌های خاص همچنین محدود کردن دیوایس در زمان خواب، مدرسه و دیگر موارد است.

این برنامه به وسیله مرورگرهای اینترنت قابل کنترل می‌باشد و همچنین به صورت پس زمینه و مخفی اجرا خواهد شد.

هر چند برخی از این برنامه‌ها امکان دخالت صریح والدین را بر کار فرزندان خود می‌دهند و سؤ استفاده از آن‌ها و دخالت بیش از حد می‌تواند نتیجه خوبی نداشته باشد اما تا زمانی که کودکان به حد کافی رشد نکنند و همچنین قرار باشد تلفن همراه و تبلت و غیره در اختیار داشته باشند، کنترل آن‌ها لازم و ضروری است.

راهکار دیگری به نام افزونه‌های فایرفاکس

افزونه‌ها بسته‌های کوچکی هستند که کارایی فایرفاکس را گسترش می‌دهند. از گزارش آب و هوا گرفته تا برنامه‌های نظارت والدین و ... می‌باشند. این افزونه‌ها در واقع تکه‌های کوچک برنامه‌اند که قابلیت‌های مختلفی را به این مرورگر می‌افزایند. با استفاده از افزونه‌های نظارت والدین در فایر فاکس می‌توانید اقداماتی مختلفی انجام دهید که هریک منحصر به یک افزونه خاص است و درر زیر به برخی از آن‌ها اشاره می‌شود:

فیلتر فایرفاکس یاFoxFilter

نحوه کار این افزونه به این شکل است که قبل از ورود شما به یک سایت، سریعاً محتوای آن را چک می‌کند و اگر مناسب تشخیص ندهد، هشدار می‌دهد. این افزونه برای پدر و مادرهایی که نگران وبگردی بچه‌هایشان هستند بسیار عالی است.

بخش چهارم: معرفی موتورهای جستجوی امن برای بچه ها

این روزها می توانید بگویید که فرزندان ما اطلاعات کافی از وب و اینترنت دارند و تا حدودی با ویژگی های این فضا آشنا هستند. با کمی کمک پدر و مادر ، آنها به راحتی می توانند اصول اولیه جستجو را درک کرده و بیاموزند . موتورهای جستجوی معمول وب به کودکان کم سن و سال همچون بزرگسالان خدمات می دهند. اما حتی در موتورهای جستجویی که فیلترهای میانه رو اعمال می شود، برخی از مطالب و محتوا ممکن است مناسب برای این ذهن های راحت تاثیر پذیر مناسب نباشد.

مرور و نمایش محتوای مناسب و مطابق با اصول اخلاقی شاید اصلی ترین دلیل برای استفاده از موتور های جستجوی به طور خاص طراحی شده برای بچه ها باشد .دلیل بعدی استفاده از این موتور های جستجو شکل ظاهری آنهاست که بیشتر با روحیات کودکان یا نوجوانان مطابقت دارد. بی شک اجازه دادن به بچه ها برای استفاده و اجرای نتایج جستجو در وب با استفاده از یک موتور جستجو ویژه بچه ها به کاهش بار نگرانی ذهنی پدر و مادر در مورد امنیت کودکان در فضای مجازی کمک شایانی می کنند.

البته ، هیچ تضمینی وجود ندارد که هر جستجویی برای کودک امن باشد، اما در وب سایت هایی که در زیر به معرفی آنها می پردازیم احتمال اینکه محتوای نمایش داده شده به کودک از مطالب ضد اخلاقی یا جاسوسی و هرزه نگاری دور تر باشد بیشتر است. گذشته از این، شما می توانید با دستکاری تنظیمات هر موتور جستجو که هر ابزار جستجویی دارای آن است به این امر کمک بیشتری کنید. از طرف دیگر شما می توانید از منابع جستجوی این ۱۰ پایگاه برای آموزش بیشتر در مورد مسائل امنیتی گشت و گذار کودک در فضای مجازی استفاده نمایید.

موتور گوگل برای کودکان

سایت Kid Rex درواقع موتور جست و جوی سفارشی گوگل برای بچه ها است. محیط صفحه اصلی درست مانند نقاشی مدادرنگی یا مدادشمعی کودکانه است (با یک دایناسور محافظ). این موتور جست و جو از شیوه های جست و جوی اخلاقی و امن استفاده می کند و حتی المقدور سعی در نمایش تمام نتایج به شکلی فاقد مطالب نامناسب برای کودک می کند.

Kid Rex همچنین دارای یک پایگاه داده ویژه حاوی سایت های نامناسب و کلمات کلیدی هرزه است که به نمایش نتایج تمیز و عاری از آلودگی بیشتر کمک می کند.

Quintura for Kids:

توسط یاهو پشتیبانی و اداره می گردد. این سایت، جستجوی تصویر جالبی را با استفاده از کلمه کلیدی به کاربر نمایش میدهد. کافیست کودک شما کار جستجو را با وارد کردن کلمه کلیدی در جعبه متن شروع کرده و سپس آن را با هر یک از کلمات کلیدی که موتور جستجو به او نمایش می دهد تغییر یا اصلاح نماید Quintura .در هر صفحه ۵ نتیجه نمایش می دهد. ممکن است به این موضوع تاکنون توجه نکرده باشید اما کلیک کردن بر روی آیکون های اطراف، شما را به ۵ دسته جستجو از پیش تعیین شده هدایت می کند: موسیقی ، تاریخ ، حیوانات ، ورزشی (تفریح و سرگرمی) و بازی.

Dib Dab Doo and Dilly Too:

اگر یک نام دامنه در سراسر وب باشد که فریاد بزند که موتور جستجو برای بچه هاست ، همین سایت است! موتور جستجوی این سایت نیزبر اساس جستجوی سفارشی گوگل بنا نهاده شده و تلاش طراحان این بوده تا انجا که ممکن است محتوای کودکانه به کاربران خود ارائه دهند.

جستجوی سفارشی به کودک کمک می کند تا از بسیاری لینک های نامناسب دور شود ، اما قطعا این امر صد درصد و در همه موارد نیست. بسیاری از موتورهای جستجو برای بچه ها نیز تبلیغاتی نمایش می دهند که بعضی از آنها نامطلوب و نامناسب و بعضا غیر اخلاقی است.استفاده از نرم افزار های کنترل والدین در ترکیب با استفاده از موتورهای ویژه جستجوی کودکان می تواند به حفظ کودکان و در امان ماندن این ذهن های پاک از جنبه های بد وب کمک شایانی نماید. این یک نبرد دشوار است ، اما با این روش ها والدین می توانند کمی کمتر نگران باشند. این موتورهای جستجو برای کودکان فقط ابزارهای جستجو برای در امان ماندن کودکان دلبندمان از مشاهده وب سایت های غیر مرتبط می باشند و باید به دیگر جنبه های محافظت از کودک در فضای انلاین نیز توجه کافی نمود.

بخش پنجم: راهکارهایی برای افزایش امنیت تلفن‌های همراه

اما امروزه با پیشرفت فناوری به خصوص پیشرفت روزافزون گوشی‌های همراه، دیگر اطلاعات ما محدود به چند پیامک و شماره های تماس نمی شوند بلکه اطلاعات شخصی یا تجاری زیادی را در این وسیله ارتباطی ذخیره می‌کنیم که می تواند تصاویر و اطلاعات خصوصی تا نامه‌های مهم، حساب‌های بانکی و شبکه‌های اجتماعی را شامل شود.

در سال‌های نه چندان دور تمامی اطلاعاتی که روی گوشی همراه ذخیره می‌شد، به تعدادی شماره و پیامک‌های متنی محدود می‌شد.اما امروزه با پیشرفت فناوری به خصوص پیشرفت روزافزون گوشی‌های همراه، دیگر اطلاعات ما محدود به چند پیامک و شماره های تماس نمی شوند بلکه اطلاعات شخصی یا تجاری زیادی را در این وسیله ارتباطی ذخیره می‌کنیم که می تواند تصاویر و اطلاعات خصوصی تا نامه‌های مهم، حساب‌های بانکی و شبکه‌های اجتماعی را شامل شود.

اگر دقت لازم را نداشته باشیم، تمامی اطلاعات ما ممکن است قابل ردیابی، دانلود و یا حتی به اشتراک گذاری در اینترنت باشد و به این ترتیب زمینه برای سرقت توسط افراد سودجو فراهم می‌شود و با توجه به این که در میان دارندگان گوشی‌های هوشمند بخش عمده‌ای مبتنی بر سیستم عامل اندروید هستند باید راهکارهایی برای جلوگیری از سرقت اطلاعات افراد در این گوشی ها ارائه کرد

نکاتی برای افزایش امنیت تلفن‌های همراه هوشمند :

۱- تمامی گذر واژه های (پسورد) خود را در گوشی ذخیره نکنید،

بسیاری از کاربران گوشی‌های هوشمند تمایل دارند گذر واژه‌های خود را برای سرویس‌های برخط و سایت‌های مختلف از جمله شبکه‌های اجتماعی، رایانامه‌ها و فروم‌ها روی تلفن هوشمند خود ذخیره کنند و حتی یک لحظه هم به این موضوع فکر نمی‌کنند که ممکن است فردی به گوشی آنها دسترسی پیدا کرده و به تمامی اطلاعات آنها نفوذ پیدا کند.

بنابراین از ذخیره‌سازی گذرواژه‌های خود به ویژه آنهایی که مربوط به حساب های بانکی یا برنامه‌های کاربردی پرداخت برخط هستند، جدا خودداری نمایید.

از گذرواژه‌های ساده که به راحتی قابل حدس زدن باشند، استفاده نشود و همچنین حروف تکراری در آنها به کار نرود. در انتخاب گذارواژه از اسم خود، تاریخ تولد، شماره ملی، شماره گواهینامه و در کل هر چیزی که مربوط به مدارک شناسایی ما می‌شود، استفاده نکنیم.

بهتر است از یک گذرواژه پیچیده و طولانی برای بالا بردن امنیت حساب‌های کاربری استفاده کنیم. گذرواژه شما باید حداقل شامل ۸ حرف و ترکیب عدد با نمادها به صورت بزرگ و کوچک باشد. هر چند وقت یک بار گذرواژه خود را تغییر دهید.

۲- از امکانات امنیتی موجود در سیستم عامل گوشی خود استفاده کنید

شما می‌توانید از قفل صفحه نمایش و رمزنگاری که در سیستم عامل اندروید وجود دارد برای افزایش امنیت خود استفاده کنید. تنوع زیادی در قفل صفحه نمایش وجود دارد که شما می‌توانید یکی از آنها را انتخاب کنید از جمله گذرواژه، پین کد، الگو(Pattern) ، تشخیص چهره، اثر انگشت که در تنظیمات سیستم عامل اندروید موجود است. پس از این که یکی از این گزینه‌ها (به جز اثرانگشت و تشخیص چهره) را برای قفل صفحه نمایش خود انتخاب کردید، سعی کنید کدها و الگوهای شما ساده و قابل حدس زدن برای هکرها نباشند.

۳- برنامه‌های کاربردی خود را قفل کنید

خیلی مهم است که برنامه‌های کاربردی خود را قفل کنید. به ویژه آن دسته از برنامه های کاربردی که اطلاعات مهمی را در آنها ذخیره کرده‌اید و مایل به افشا شدن آنها نیستید.

این کار در واقع لایه دوم امنیتی است که در صورتی که دستگاه شما در اختیار شخص دیگری به ویژه به هنگام گم شدن آن قرار گیرد، مانع از افشای اطلاعات شما حتی پس از عبور از قفل صفحه نمایش می‌شود. برای قفل نمودن برنامه‌های کاربردی خود می‌توانید از برنامه کاربردی ویژه استفاده کنید.

۴ – مجوزهای مورد درخواست برنامه‌های کاربردی را در هنگام نصب به دقت بخوانید

پیش از اینکه برنامه کاربردی دریافت شده خود از فروشگاه معتبر گوگل (Google Play) یا اپل (App Store) و یا کندو (Cando)را روی تلفن همراه هوشمند نصب نمایید، یک لیست از درخواست‌های دریافت مجوز که برنامه کاربردی نیاز دارد، برای شما ظاهر خواهد شد.

برنامه های کاربردی نیازمند یکسری مجوز هستند تا به وظایف خود عمل کنند اما همه مجوزهای درخواستی ضروری نیستند.

همیشه پیش از اتمام مراحل نصب یک برنامه کاربردی تمامی مجوزهای درخواستی را مطالعه نمایید تا مطمئن شوید مجوزها مربوط به کارهایی است که واقعاً آن برنامه کاربردی باید انجام دهد.

به عنوان مثال، یک برنامه کاربردی چراغ قوه نیازمند مجوز دسترسی به پیام های متنی شما نیست! این گام یک گام بسیار مهم و ضروری برای افزایش امنیت گوشی هوشمند شما است زیرا همه برنامه های کاربردی موجود در فروشگاه گوگل ایمن نیستند و برخی از آنها شامل بدافزارهای جاسوسی و کدهای مخرب هستند.

هنگامی که می خواهید یک برنامه کاربردی را دریافت کنید حتماً نظرات کاربران را در مورد آن برنامه کاربردی مطالعه کنید و سپس به دریافت آن اقدام نمایید. این کار باعث می‌شود تا شما اطلاعات بیشتری در مورد برنامه کاربردی موردنظر خود داشته باشید.

۵ – ایمن سازی شبکه ارتباطی

یکی از مهم‌ترین مواردی که امنیت گوشی شما را تأمین می‌کند، ایمن بودن شبکه ارتباطی شماست. از اتصال به ارتباطات بی‌سیم عمومی جدا خودداری کنید. به ویژه هنگامی که می‌خواهید کارهای بانکی خود را از طریق اینترنت انجام دهید.
هنگامی که شما به یک شبکه بی‌سیم عمومی متصل می‌شوید، آنها می‌توانند به راحتی بسته‌های ارسالی شما را شنود کرده و آنها را به داده‌های اصلی ترجمه نمایند که این داده‌ها می توانند اطلاعات خصوصی و گذرواژه های شما باشند.

۶ – از برنامه‌های کاربردی امنیتی موبایل (ضدویروس‌ها) استفاده کنید
داشتن یک برنامه کاربردی از نوع ضدویروس کار شما را در تأمین امنیت دستگاه راحت تر می‌کند. یک برنامه کاربردی امنیتی که استفاده از آن ساده باشد، انتخاب و اقدام به نصب آن کنید.

۷ – با ایجاد چند حساب کاربری از حریم خصوصی خود محافظت کنید

اگر شما دارنده یک تبلت هستید و می‌خواهید آن را با خواهر، برادر، همسر و یا فرزند خود به اشتراک بگذارید ایجاد چند حساب کاربری به شما در حفظ حریم خصوصی خود و دیگران کمک خواهد کرد.
در نسخه‌های جدید سیستم عامل اندروید گزینه ایجاد حساب‌های کاربری وجود دارد و همچنین شما می‌توانید با ایجاد یک حساب کاربری عمومی برای هر کسی که می‌خواهد از دستگاه شما استفاده کند، محدودیت دسترسی به اطلاعات ایجاد کنید.
شما می‌توانید در قسمت Settings وارد بخش Users شوید تا از این قابلیت سیستم عامل اندروید بهره‌مند شوید.

۸ – یک نسخه پشتیبان از داده‌های خود تهیه کنید

یک نسخه پشتیبان از داده‌های دستگاه شما می‌تواند مربوط به یک بازه زمانی طولانی از داده های جمع‌آوری شده باشد. تصور اینکه دستگاه شما به سرقت رفته و یا هک شده باشد بسیار بد و دلخراش است.
تنها کاری که باید انجام دهید، این است که از راه دور اطلاعات خود را از روی دستگاه پاک کنید (توضیح در بخش ۱۰) و اگر از آن اطلاعات پشتیبان گیری نکرده باشید، تمامی اطلاعات خود را از دست خواهید داد.
در صورتی که توانسته باشید دستگاه به سرقت رفته خود را دوباره به دست آورید، باز هم ممکن است دستگاه در زمان سرقت دستکاری شده باشد و اطلاعات شما توسط هکرها مورد حمله قرار گیرد.

شما می‌توانید با پشتیبان گیری و بازگرداندن دستگاه اندرویدی خود به وضعیت اولیه، با این تهدید نیز مقابله نمایید.

۹ – ردیابی دستگاه گم شده

علاوه بر داشتن پشتیبان، شما باید قابلیت ردیابی دستگاه به سرقت رفته و یا گم شده خود را داشته باشید. خوشبختانه گوشی‌های هوشمند دارای فناوری ردیابی هستند که به وسیله GPS این قابلیت برای آنها امکان‌پذیر خواهد بود.
برای دریافت آن شما باید سیستم موقعیت یاب جهانی موجود در گوشی خود را فعال نموده تا بتوانید آن را ردیابی کنید.
برنامه‌های کاربردی زیادی از جمله AntiDroidTheft برای یافتن دستگاه به سرقت رفته و یا گم شده شما وجود دارند که برخی از آنها قابلیت روشن کردن GPS از راه دور را نیز دارند.

۱۰ - فعال نمودن بخش پاک سازی از راه دور

پس از انجام مراحل بالا، تقریباً دستگاه شما از امنیت مناسبی برخوردار خواهد بود. اما یک گام دیگر باقی خواهد ماند و آن قابلیت حذف اطلاعات دستگاه از راه دور است.
این موضوع برای فردی که دیگر امیدی به بازگشت دستگاه خود ندارد بسیار مهم است که توانایی حذف داده‌های شخصی و محرمانه خود را از راه دور داشته باشد.
برای این کار برنامه‌های کاربردی زیادی وجود دارند که ۳ CX Mobile Device Managerیک برنامه رایگان و با واسط کاربری ساده نیاز شما را برآورده خواهد کرد.

توصیه‌های امنیتی برای استفاده کودکان از تلفن همراه

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای، نسبت به تهدیدات امنیتی در استفاده کودکان از تلفن های همراه هشدار داد و نکاتی را برای مقابله والدین با این تهدیدات اعلام کرد .
امروزه استفاده از تلفن همراه در بین کودکان در حال افزایش است؛ به همین دلیل آموزش مناسب والدین به فرزندان خود در خصوص استفاده ایمن از تلفن همراه و کنترل کردن فعالیت های کودکان می تواند تا حدی با تهدیدات امنیتی مقابله کند.

ماهر از والدین خواست تا هر زمان که فرزندانشان برای استفاده از تلفن هوشمند آماده بودند، به آنها در خصوص ایمنی و مسئولیت پذیری آموزش‌های لازم را ارائه دهند.

دسترسی کودکان را محدود کنید

تلفن همراه و شرکت‌های تلفن سیار (wireless company) معمولا امکاناتی را در خصوص تنظیمات حریم خصوصی و کنترل‌های ایمنی کودک ارائه می‌دهند. اکثر شرکت‌ها به والدین امکان خاموش کردن قابلیت‌هایی مانند دسترسی وب، ارسال پیام کوتاه یا دانلود کردن را می‌دهند.

برخی تلفن‌های همراه سلولی، خاص کودکان ساخته شده‌اند. این تلفن‌ها برای استفاده ساده طراحی شده و دارای قابلیت‌هایی مانند دسترسی محدود به اینترنت، مدیریت دقیقه(minute management) ، حفظ حریم خصوصی شماره‌ها، و دکمه‌های تماس اضطراری هستند.

الزام استفاده از تلفن‌های محافظت شده با کلمه عبور

کلمه عبور، کد عددی یا اثر انگشت می‌تواند منجر به عدم دسترسی مزاحمان به تلفن شود. این کار نه تنها می‌تواند از «تماس تصادفی (pocket dialing)» جلوگیری کند بلکه می‌تواند به حفظ اطلاعات و عکس‌ها در برابر دسترسی افراد غیرمجاز کمک کند.

هنگام به اشتراک گذاری تصاویر و ویدئوها مراقب باشید

به اشتراک گذاری و اجتماعی بودن می‌تواند فرصت‌ها و چالش هایی را ایجاد کند. این ابزارها می‌تواند باعث ایجاد خلاقیت و سرگرمی کودک شود اما از طرفی دیگر می‌تواند منجر به بروز مشکلاتی در خصوص اعتبار و ایمنی اشخاص شود.

بیشتر تلفن‌های همراه قابلیت عکس گرفتن و تصویربرداری را دارند و به اشتراک گذاری و گرفتن تصاویر را در هر لحظه آسان می‌کنند.

فرزندانتان را تشویق کنید که در خصوص حفظ حریم خصوصی خود و دیگران قبل از به اشتراک گذاری تصاویر و فیلم‌ها از طریق تلفن همراه فکر کنند.

قبل از ارسال تصاویر یا فیلم‌ها، از کسی که در تصویر یا فیلم است اجازه بگیرند. اینکه از ابتدا به اندازه کافی هوشمند باشیم که چه تصویر یا فیلمی به اشتراک گذاشته شود نسبت به اینکه بعدا بخواهیم خسارت را کنترل کنیم ساده‌تر است.

استفاده از اپلیکیشن ها را محدود کنید

اپلیکیشن ها و برنامه های کاربردی ممکن است اطلاعات شخصی را جمع آوری و به اشتراک بگذارند، ممکن است رایگان باشند اما فرزندان شما را ترغیب به پرداخت پول کنند و یا شامل تبلیغات باشند و به رسانه‌های اجتماعی (social media)متصل باشند، اما این برنامه‌ها ممکن است به شما درباره کارهایی که انجام می دهند چیزی نگویند؛ براین اساس کارهایی وجود دارند که شما و فرزندتان می توانید قبل از دانلود برنامه برای یادگیری درباره برنامه های کاربردی انجام دهید.

تصاویر انتشاریافته از این برنامه را بررسی کنید، توضیحات مربوطه، رده بندی محتوایی، و نظرات کاربران را بخوانید، درباره توسعه دهنده برنامه تحقیق کنید و بررسی کنید که برنامه کاربردی چه اطلاعاتی را جمع آوری می کند.

شما می توانید چگونگی استفاده از اپلیکیشن ها توسط کودکان را محدود کنند؛ به نحوی که قبل از اینکه تلفن یا تبلت خود را به فرزندتان بدهید، به تنظیمات آن نگاه کنید.

محتوا را به آنچه که مناسب سن کودک شما است محدود کنید، کلمه عبوری را تنظیم کنید که برنامه های کاربردی بدون آن نتواند دانلود شوند و کودکان نتوانند بدون آن چیزی بخرند، همچنین خدمات داده و وای فای را خاموش کنید تا به اینترنت متصل نشوید. همچنین می توانید تلفن را در حالت پرواز قرار دهید.

درهمین حال بهترین راه برای مراقبت در قبال برنامه‌های کاربردی کودکان تست و بررسی توسط والدین است. با فرزندان خود درباره قوانین خرید و استفاده از این برنامه های کاربردی صحبت کنید.

از حریم خصوصی کودکان خود محافظت کنید

به کودکان خود یادآوری کنید که متن‌هایی که از افراد ناشناس دریافت می کنید نادیده بگیرند؛ یاد بگیرند که چگونه شماره هایی را در تلفن همراه خود مسدود کنند، از ارسال شماره تلفن خود به صورت آنلاین اجتناب کنند، هرگز اطلاعات شخصی یا مالی خود را در پاسخ به پیامکی ارائه ندهند.

کودکان باید پیامک هرزنامه ای را تشخیص دهند؛ به فرزندان خود در تشخیص پیامک هرزنامه ای کمک کنید و نتایج این نوع پیامک ها را توضیح دهید. این پیامک ها اغلب وعده هدایای رایگان را می دهند یا از شما خواسته می شود که اطلاعات کاربری خود را تایید کنید تا از این طریق شما اطلاعات شخصی تان را آشکار کنید؛ این پیامکها همچنین می توانند منجر به شارژ هزینه های ناخواسته در صورتحساب تلفن همراه شما شوند و می توانند کارایی تلفن همراه شما را پایین بیاورند.

مقابله با تهدیدات امنیتی موبایل

خانواده ها میتوانند صورتحساب تلفن همراه خود را بررسی کرده و ببینند آیا هزینه های غیرمجازی در صورتحساب خود مشاهده می کنند و یا خیر .همچنین به فرزندان خود بگویند پیام هایی را که اطلاعات شخصی را درخواست می کند حذف کنند، حتی اگر وعده هدیه رایگان را می دهد.

باید توجه داشت که شرکت های قانونی اطلاعاتی مانند شماره حساب ها یا کلمات عبور را از طریق ایمیل یا متن درخواست نمی کنند؛ براین اساس به لینک هایی که در پیامک می آید پاسخ ندهید و روی آنها نیز کلیک نکنید؛ لینک ها می توانند بدافزاری را نصب کنند و شما را به سمت سایت های کلاهبرداری ببرند که اطلاعات شما را به سرقت ببرند .

فصل ششم: پرداخت الکترونیک امن

صفحه کلید امن :

صفحه کلید امن برای وارد کردن اطلاعات در داخل فیلدها در نظر گرفته شده است، این صفحه کلید موارد امنیتی لازم را در هنگام پرداخت اینترنتی برای شما فراهم می کند. اگر برای پر کردن اطلاعات کارت از این صفحه کلید استفاده کنید برنامه های Key logger قادر به ذخیره کردن شماره کارت و رمز اینترنتی شما نخواهند شد . Key loggerبرنامه ایست که به محض اجرا بر روی سیستم اعداد فشرده شده توسط کاربر را در خود ذخیره می کند و این باعث می شود که امنیت اطلاعات وارد شده از جانب شما به خطر بیفتد و این اطلاعات در آینده مورد سوء استفاده قراربگیرند. از آنجایی که در صفحه کلید امن محل قرارگیری کلید ها در هر بار لود شدن صفحه تغییر می کند امکان تشخیص کلید های فشرده شده وجود ندارد. در نتیجه برای حفظ امنیت بیشتر پیشنهاد می کنیم که از این صفحه کلید برای ورود اطلاعات کارت استفاده کنید.

پس از آنکه موارد ذکر شده را وارد کردید منتظر بمانید تا پرداخت اینترنتی شما تایید گردد و در همان لحظه مبلغ از حساب شما کسر گشته و مجددا به سایت فروشنده باز میگردید و ادامه مراحل خرید را انجام خواهید داد.

مشکلات احتمالی پرداخت اینترنتی

سیستم پرداخت اینترنتی توسط بانک های عامل به گونه ای طراحی شده است که هم ایمن باشد و هم ساده و کمترین نیاز به راهنمایی را برای خریدار ایجاد نماید. لکن در صورتی که در طی فرایند خرید اینترنتی مغایرتی به وجود آید ، مثلاً ممکن است در هنگام پرداخت شبکه بانکی قطع شود و پرداخت ناموفق انجام شود.

معمولاً بدترین حالتی که ممکن است به وقوع بپیوندد این است که پول ازحساب شما کسر شود، ولی به حساب فروشنده واریز نشود. اما نگران نباشید. در این حالت معمولاً پول شما در حساب های حد واسط بانک است. نهایتاً خود بانک می باید مغایرت ها را رفع کند. منتظر بمانید و اگرتا ۴۸ ساعت پول به حسابتان برگشت نخورد، آنگاه مشتریان محترم می توانند از طریق بانک عامل تراکنش نا موفق خود را پیگیری و اعلام مغایرت نمایند.

نکات امنیتی در پرداخت های الکترونیکی

۱. رمز خود را جایی یادداشت نکنید و در صورت یادداشت نمودن، آن را در جیب یا کیف پول به همراه کارت قرار ندهید.
۲. رمزهای عبور خود را به صورت دوره ای تغییر دهید.
۳. رمز خود را در اختیار سایر افراد قرار ندهید.
۴. اطلاعات حساس از جمله رمز خود را از طریق تلفن برای دیگران بازگو نکنید.
۵. در صورت فاش شدن رمز خود، در کوتاهترین زمان ممکن آن را عوض نمایید.
۶. کارت و رمز خود را به هیچ وجه در اختیار دیگران قرار ندهید. بعضاً افراد سود جو به بهانه کمک کردن و راهنمایی ضمن اخذ کارت و رمز شما پس از انجام عملیات، کارت شما را با کارت دیگری (سرقتی ، مفقودی ، باطله و...) معاوضه نموده و حساب شما را مورد سوء استفاده قرار می دهند.
۷. در صورت انجام انتقال وجه و عملیات اینترنتی برروی حساب خود در مرورگرهای اینترنت گزینه ی به خاطرسپردن رمز را انتخاب نکنید. این گزینه با نام کلی Remember Password شناخته می شود، از این قابلیت استفاده نکنید.
۸. برای ارسال اطلاعات حساس خود از پست الکترونیکی استفاده ننمایید.
۹. همواره سعی کنید برای ورود رمز خود از امکان Virtual Keyboard بجای کیبورد فیزیکی کامپیوتر استفاده کنید. این امکان در سیستم عامل ویندوز و همچنین در برخی از سایتهای پرداخت آنلاین وجود دارد.
۱۰. شناسه عبور و رمز خود را بر روی کامپیوترهای خارج از اختیار و کنترل خود وارد نکنید.

۱۱. هنگام ورود به وب سایتها به ویژه وب سایتهایی که در آن اطلاعات محرمانه وارد می گردد، آدرس سایت مورد بازدید را در کادر نوار آدرس کنترل نمایید. بسیاری از کلاهبردارهای اینترنتی بواسطه استفاده از سایتهای جعلی و مشابه، جهت دریافت اطلاعات حساس کابران رخ می دهد.

۱۲. همواره از سایت ای خرید نمایید که دارای لوگوی نماد اعتماد الکترونیکی مرکز توسعه تجارت الکترونیکی ایران میباشد.

۱۳. در صفحاتی که سایت مورد بازدید از شما درخواست ورود شماره کارت، رمز کارت، رمز دوم و CVV2 می نماید، حتماً مطمئن شوید که از پروتکل SSL استفاده شده است. بدین منظور آدرس صفحه می بایست با عبارت https بجای http آغاز گردد.

۱۴. همواره از نرم افزارهای آنتی ویروس معتبر و بروزشده استفاده نمایید.

۱۵. سیستم عامل کامپیوتر خود را همواره بروزرسانی کرده و آخرین وصله های امنیتی را دریافت نمایید.

۱۶. در صورتی که احتمال وجود برنامه های مخرب را بر روی کامپیوتر خود می دهید از انجام هرگونه تراکنش مالی آنلاین خودداری نمایید.

۱۷. پس از انجام کار مورد نیاز در وب سایتهایی که نیاز به رمز ورود دارند، به طور کامل Log out کنید.

۱۸. به مطالب نوشته شده در پنجره هایی که اتوماتیک نمایش داده می شوند توجه نموده و بلافاصله بر روی Ok یا Yes کلیک نکنید. بسیاری از برنامه های مخرب به همین شیوه بر روی کامپیوترها نصب می گردند.

۱۹. ایمیلهای دریافتی از منابع ناشناس را باز نکنید. به لینکهای ارائه شده در ایمیلها اعتماد نکنید، به عنوان نمونه بانکها و موسسات اعتباری هیچ گاه از طریق نامه های الکترونیکی اطلاعات محرمانه شما را درخواست نمی کنند. بنابراین هرگاه در صندوق پستی خود نامه هایی از این دست را مشاهده کردید به سرعت آن را حذف کنید. از داده های حساس خود نسخه پشتیبان تهیه نموده و در جایی امن نگهداری کنید.

۲۰. برای پرداخت های الکترونیکی بهتر است از رایانه های شخصی به جای رایانه های موجود در اماکن عمومی و کافی نت ها استفاده کنند

۲۱. ضمناً لازم است کاربران در انتخاب کلمه عبور و رمز دوم کارت دقت کافی را داشته باشند، بدین صورت که کلمات عبور به صورت ترکیبی از حروف کوچک و بزرگ و اعداد و علائم مجازی انتخاب شوند.

۲۲. تا حد امکان از وای‌فای‌های عمومی استفاده نکنید بدون شک، وای‌فای های عمومی یکی از امکاناتی است که همه ما به هنگام حضور در کافی‌شاپ‌ها، رستوران‌ها و یا سایر اماکن انتظار داریم موجود باشد. اما زمانی که صحبت از خرید برخط می‌شود، استفاده از این نوع وای‌فای‌ها توصیه نمی‌شود. استفاده از چنین اتصال‌هایی

به هنگام خرید برخط ممکن است تحت حملات نفوذگران منجر به سرقت اطلاعات حساب شما شود. یکی از انواع حملات رایج، حملات مردمیانی است که اغلب با هدف سرقت اطلاعات بانکی در اماکن عمومی راه‌اندازی می‌شود.

۲۳. مراقب پیشنهادهای وسوسه کننده باشید احتمالاً برای همه ما پیش آمده‌است که با پیشنهاد باورنکردنی در محیط برخط مواجه شده‌ایم که با اشتیاق آن را دنبال کرده‌ایم تا شاید احتمالاً شانس این را داشته باشیم محصولی را با کسری از قیمت واقعی آن بخریم! اما این اتفاق واقعاً نادر است. باید مراقب بود، چرا که همیشه کلاهبردارانی در کمین‌اند تا با همین پیشنهادات اغوا کننده شما را گول بزنند. توصیه می‌شود به هنگام نزدیک شدن به تعطیلات مهم مانند تطعیلات سال نو که معمولاً آمار خرید بالا می‌رود، و تعداد این‌گونه پیشنهادات بیش‌تر هم می شود، بیش‌تر نیز مراقب باشید.

نکات امنیتی برای انجام عملیات بانکی با استفاده از تلفن همراه

در طی سال‌های اخیر اکثر بانک ها اقدام به تولید و عرضه نرم افزارهای بانکداری مخصوص تلفن های همراه و سایر دستگاه‌های کامپیوتری قابل حمل کرده اند؛ اما اگر تلفن شما به سرقت برود، چه اتفاقی خواهد افتاد؟ آیا سارق می تواند از تلفن همراه شما برای خالی کردن حساب بانکی شما استفاده کند؟

با توجه به این‌که تمایل به استفاده از نرم افزارهای بانکداری رشد بسیار سریع در بخش مالی داشته است، رعایت نکات امنیتی و اقدامات احتیاطی جهت پیشگیری از کلاهبرداری از حساب‌های بانکی، لازم و ضروری است از جمله این اقدامات نصب نرم افزارهای ضد ویروس است که برای تضمین امنیت انتقال پول الکترونیکی شما مفید خواهد بود، استفاده کنندگان از این نرم افزارها، باید همان اقداماتی را انجام دهند که در هنگام استفاده از یک کامپیوتر شخصی برای انجام عملیات بانکی خود انجام می دهند .

نرم افزارهای بانکداری قابل نصب روی تلفن های همراه امکانات زیادی را فراهم کرده اند،به گونه ای که افراد پر مشغله، برای انجام امور بانکی خود از این نرم‌افزارها استفاده می کنند؛اما استفاده کنندگان از این نرم افزارها باید نکات امنیتی را رعایت کرده و از گذرواژه‌های قوی استفاده کنند تا اگر تلفن آن‌ها به سرقت رفت، بتوانند، امنیت پول خود را تضمین کنند.

اگر کاربران اقدامات احتیاطی لازم را انجام ندهند، امکان کلاهبرداری از بسیاری از کاربران وجود دارد .

به استفاده کنندگان از این نرم افزارها پیشنهاد می کنیم، نکات زیر را رعایت کنند:

۱. نرم افزارهای ضد ویروس را بر روی تلفن همراه خود نصب کنید تا اگر برنامه یا محتوایی را دانلود می کنید، از دستگاه خود در برابر ویروس ها و نرم‌افزارهای مخرب محافظت کنید؛

۲. گذرواژه‌ها، اطلاعات شخصی و شماره حساب های بانکی خود را محرمانه نگه دارید. این اطلاعات را در اختیار هیچ شخصی قرار ندهید؛مگر آن‌که خود شمااقدام به برقرار ارتباط کرده باشید و مطمئن باشید که با بانک یا نرم افزار ارائه شده از طرف بانک کار می کنید؛

۳. گذرواژه‌ها، شماره رمز عبور شخصی(PIN) ، و پاسخ‌های مربوط به سوالات محرمانه نرم افزار یا شماره حساب های بانکی تان را در دستگاه خود ذخیره نکنید. اطمینان حاصل کنید که از گذر واژه‌های قوی که شامل ارقام، علائم و حروف است، استفاده می کنید؛

۴. تلفن همراه یا دستگاه خود را به گونه ای تنظیم کنید تا وقتی که دستگاه روشن می شود از کاربر گذر واژه بخواهد. هیچ گاه دستگاه خود را به گونه ای تنظیم نکنید که به صورت خودکار با حساب بانکی ارتباط برقرار کند.

۵. به پیام‌های متنی که از شما شماره حساب بانکی تان را می‌خواهند، پاسخ ندهید. تصور کنید که هر پیام ناخواسته و ناآشنا به قصد کلاهبرداری از شما ارسال شده است. بانک شما هرگز با ارسال پیام متنی با شما ارتباط برقرار نخواهد کرد؛

۶. اگر تلفن همراه شما گم شد یا به سرقت رفت، مراتب را فوراً به شرکت ارائه دهنده خدمات تلفن همراه و بانک عاملی که خدمات مربوطه را پشتیبانی می کند، اطلاع دهید.

فصل هفتم : مسدود کردن پورت های غیرضروری

از آنجایی که امنیت سایبری کاربران برای ما مهم می باشد لازم است در مورد پورت های مهم و غیرضروری که هکرها از طریق آنها امکان نفوذ به شبکه شما را خواهند داشت توضیح دهیم.

متاسفانه با بررسی های انجام شده مشاهده می شود که در شبکه اینترنت حفره های امنیتی بسیاری موجود است که باعث ایجاد اختلال برای عده ای از کاربران خواهد شد.

به صورت روزانه هکرهایی در شبکه جهانی اینترنت مشغول جست و جو و یافتن پورت هایی هستند که می توانند از آن ها سوء استفاده کرده و با آن به مقاصد نادرست خود برسند.

به طور مثال یکی از این پورت ها که می تواند احتمال سوء استفاده را برای این هکرها ایجاد کند پورت ۵۳ و به همراه آن فعال بودن قابلیت Open Relay است.

در این حالت با توجه به باز بودن پورت UDP 53 روی سرویس شما و پاسخگو بودن سرویس DNS به تمام کویری ها، هکرهای فعال در شبکه اینترنت از سرویس شما برای حمله به سمت سرورهای اینترنتی استفاده کنند و این موضوع ممکن است بدون اینکه شما در جریان باشید مشکلاتی را برای شما به عنوان مسئول و مالک سرویس ایجاد کند.

از آنجایی که در اغلب موارد مشاهده شده علت این نفوذها مسدود نکردن پورت های غیرضروری می باشد پیشنهاد می شود برای حل این مشکلات بر روی مودم ADSL خود پورت ذکر شده و سایر پورت های غیرضروری را در سیستم خود غیرفعال کنید.

تعدادی از پورت های ضروری که همیشه باید باز باشند به همراه کاربرد آن ها در جدول زیر به طور نمونه ذکر شده است:

شماره پورت	کاربرد	توضیحات
۸۰	HTTP	مربوط به باز کردن صفحات اینترنتی
۵۳	DNS LOOKUP	پورت مربوط به سرویس DNS جهت باز کردن سایت ها
۱	ICMP	مربوط به دستور PING
۲۵	SMTP	پورت مربوط به ایمیل
۱۱۰	POP3	پورت مربوط به ایمیل
۴۴۳	HTTPS	مربوط به بازکردن صفحات اینترنتی سایت های امن شده