جلوگیری از کلاهبرداری ها

کلاهبرداری عبارت از یک عمل خیانتکارانه برای فریب کسی به روشی است که به قیمت شخص فریب داده شده از لحاظ مالی به شخصیکه این عمل نادرست انجام میدهد مفاد برسد. دانستن چند نوع کلاهبرداری مهم است و اینکه چگونه متوجه آن ها شوید.

کلاهبرداری های معمولی

در زیر چهار نمونه از کلاهبرداری های رایج آورده شده است. صدها نوع دیگر وجود دارد. به طور کلی، مراقب آن تماس ها، ایمیل ها یا متونی که پیشنهادهایی را ارائه می دهند که آنقدر خوب است که باورکردنش سخت است، تهدید آمیز یا تهمت زدن، پر از خطاهای املایی و دستوری باشد، یا اطلاعات شخصی قابل تشخیص (PII) را درخواست کنند.

برنده شدن های غیر منتظره

در این کلاهبرداری ها، به شخصی که فریب داده می شود تماس گرفته می شود و به آنها گفته می شود که در رقابتی که در آن شرکت نکرده اند، پول، جنس یا خدمات را بدست آورده اند. از آنها درخواست میشود که پول یا PII ارسال کنند تا صاحب برد خود شوند. این برنده شدن ها هرگز به حقیقت تبدیل نخواهد شد. با استفاده از PII،شخصی که این فریب را بازی می کند می تواند به حساب بانکی شما دسترسی پیدا کند و پس انداز شما را به حساب شخصی خود انتقال دهد.

موسسات خیریه جعلی

در این کلاهبرداری ها، با شخص که فریب داده میشود از طرف شخصی که وانمود می کند نماینده موسسه خیریه است تماس صورت میگیرد، کسیکه بعداً پول درخواست میکند. همواره برای تأیید اعتبار آنها، موسسات خیریه را به صورت آنلاین جستجو کنید و فقط از راه های اهدای ایمن برای اهدا پول استفاده کنید.

مالیات سابقه

در این کلاهبرداری ها، شخص فریب خورده توسط شخصی که ادعا می کند نماینده خدمات درآمدهای داخلی (IRS) یا ریاست دولتی دیگر است، فراخوانده می شود و مورد تهدید دستگیری یا تبعید قرار داده میشود مگر اینکه هزینه ای پرداخت کند. IRS هرگز برای درخواست PII تماس نمی گیرد، بنابراین هیچ چیزی ارائه ندهید! در صورت دریافت این نوع تماس، شماره تلفن تماس گیرنده را در براوزر جستجوی انترنتی خود جستجو کنید. این به شما کمک می کند یاد بگیرید که قبلاً این شماره به عنوان کلاهبرداری گزارش شده باشد یا خیر. اگر نگران هستید، حادثه را به مدیر قضیه خود گزارش دهید.

پیشنهاد وظیفه غیر منتظره

در این کلاهبرداری ها، با شخص که فریب داده میشود از طرف یک شرکت جعلی تماس گرفته می شود که قبلاً مصاحبه حضوری یا درخواست رسمی به آنها نکرده است، شغل پیشنهاد می دهد. هرگز PII خود را بدون تأیید صحت مشروعیت آنها، به کارفرمای بالقوه ندهید.

معلومات شخصی قابل تشخیص چیست؟

معلومات شخصی قابل تشخیص (PII) هر نوع معلوماتی است که می تواند به طور خاص یک شخص را شناسایی کند. این شامل، اما نه محدود به، موارد ذیل میباشد:

- شماره تأمینات اجتماعی
- نام کامل
- تاریخ تولد
- آدرس ها
- شماره های حساب بانکی

برخی نشانی های یک پیام کلاهبرداری کدام ها اند؟

- لهجه غیر رسمی
- درخواست برای کارت پیش پرداخت

دیگر چه؟

HIAS

نظارت بر اطفال

به عنوان والدین در عصر دیجیتال، نظارت بر فعالیت آنلاین فرزندان شما می تواند دشوار باشد. مهم است که اطفال را در معرض اینترنت قرار دهید، که این بخشی از زندگی اجتماعی، آموزشی و حرفه ای آنها خواهد بود. در عین حال، **محافظت از کودکان در برابر جنبه های مضر اینترنت، از جمله حمله سایبری، محتوای نامناسب، سوءاستفاده مالی و شکارچیان آنلاین حائز اهمیت است**. کنترل والدین و ابزارهای نظارت برای محافظت از فرزندان شما ضروری است.

اصطلاحات کلیدی

نرم افزار جدید Android و iOS (Apple) دارای موارد کنترول برای والدین می باشند. برنامه های کنترل اضافی والدین به صورت رایگان یا خرید در سیستم عامل های نصب برنامه در دسترس هستند *(برای اطلاعات بیشتر در مورد فروشگاه های برنامه، بررسی کنید 1.1.)*

حمله سایبری (Cyberbullying)

حمله سایبری عبارت از ارسال، پست، یا شریک ساختن مطالب منفی، مضر یا کاذب در مورد شخصی است که در پیام رسانی متنی، برنامه ها، رسانه های اجتماعی، انجمن ها یا بازی هایی که افراد می توانند مطالب را با دیگران مشاهده نمایند، اشتراک کنند یا شریک می سازند می باشد.

شکارچیان آنلاین

شکارچیان آنلاین کاربران آنلاین بالغ هستند که به دنبال سوء استفاده از کودکان با استفاده از تکنولوژی دیجیتال برای یافتن و هدف قرار دادن افراد زیر سن قانونی هستند.

فیلتر محتویات

این ابزار ها دسترسی اطفال را به محتویات نامناسب محدود میسازد. فیلتر محتویات در بسیاری از برنامه ها، دستگاه ها، و براوزرها موجود می باشند.

کنترل استفاده

این کنترل ها زمان دسترسی کودکان به برنامه های خاص، ساعاتی را که در آن از برنامه های خاصی استفاده می کنند و اینکه آیا آنها به نحوی میتوانند به برنامه ها دسترسی داشته باشند، محدود می کنند.

ابزارهای نظارتی

این ابزارها به والدین امکان می دهد مکان دستگاه ها را ردیابی کنند، ببینند کودکان با دستگاه های خود چه کاری انجام می دهند و در مورد سایر جنبه های استفاده از آنها نیز یاد بگیرند.

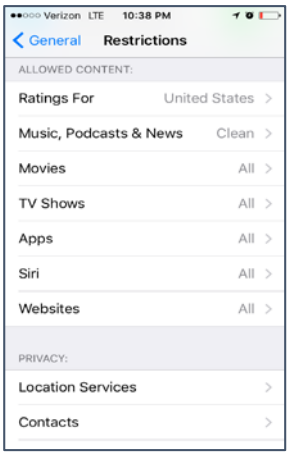
در پی جستجوی چه چیز باشیم

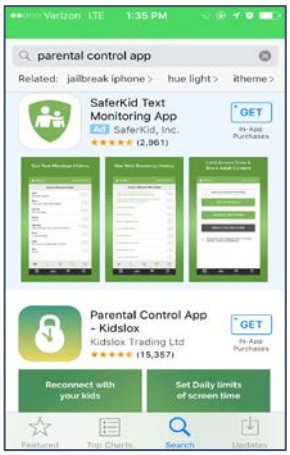
شیوه های زیادی وجود دارند که اطفال، و جوانان میتوانند در انترنت مورد سوء استفاده قرار گیرند. به عنوان والدین، دانستن در مورد حمله سایبری و شکارچیان آنلاین می تواند به شما درجلوگیری از این امر کمک کند.

بسیاری برنامه ها و بازی ها دارای خریداری های درون برنامه ای می باشند. اینها به کودکان اجازه می دهد تا خریداری های واقعی مالی انجام دهند. در صورت امکان، با به روزرسانی تنظیمات کنترل والدین از خرید درون برنامه ای جلوگیری کنید و از پیوند دادن اطلاعات بانکی خود به فروشگاه برنامه جلوگیری کنید.

محتویات خشونت آمیز، جنسی یا محتویات نامناسب به طور گسترده در انترنت قابل دسترسی است. قبل از اینکه به فرزندانتان اجازه دهید از آنها استفاده کنند، در معرض قرارگرفتن فرزندتان از طریق مرور وب سایت ها، بازی ها و برنامه ها محدود کنید.

می توان میزان قرار گرفتن فرزندتان در برابر محتویات مضر محدود ساخت، اما به طور کامل از آن جلوگیری کرده نمیتوانید. **اطمینان حاصل کنید موضوع ایمنی انترنت را طور مستقیم با اطفال تان صحبت کنید.** بسیاری از این مهارت ها در سایر جنبه های زندگی آنها مفید خواهد بود.





HIAS

مدیریت آثار فعالیت های دیجیتالی شما

آثار فعالیت های دیجیتالی شما رکورد الکترونیکی هر کاری است که در انترنت انجام می دهید. **هر پیام متنی، ایمیل، پست در رسانه های اجتماعی، تصویر، خرید و جستجوی انترنتی برای همیشه ذخیره می شود.** برای این آثار فعالیت های دیجیتالی دو لایه وجود دارند. اولین لایه اطلاعاتی است که توسط هر کاربر اینترنتی قابل دسترسی است. دوم، اطلاعاتی است که از طرف ارائه دهنده خدمات انترنت شما، شرکت ها، دولت ها و مجرمان سایبری قابل دسترس باشد. درک این مسئله که چگونه این اطلاعات جمع آوری شده، چه کارهایی با آن انجام می شود و چگونه می توان آن را مدیریت کرد، مهم است.

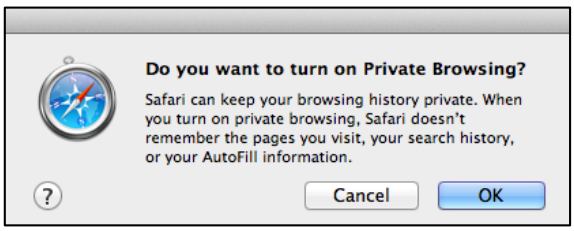
اصطلاحات کلیدی

تبلیغات هدفمند
بسیاری از وب سایت ها برای تبلیغ محصولات از وب سایت هایی که قبلاً بازدید کرده اید، از آثار فعالیت های دیجیتالی شما استفاده می کنند.

شبکه خصوصی مجازی (VPN)
یکVPN با ایجاد یک شبکه خصوصی از یک اتصال اینترنتی عامه، به شما محرمیت آنلاین ارائه می دهد. VPN کمک می کند تا مجرمان سایبری اطلاعات را که از دستگاه خود می فرستید و دریافت می کنید جلوگیری کنند. اکثر روتر های انترنتی دارای VPN خودی می باشد. تنظیم نمودن یک VPN هزینه کوچک ماهانه در بر خواهد داشت (*برای معلومات بیشتر درمورد روتر ها، بررسی کنید 1.2*).

گردش خصوصی (حالت گمنام)
هنگامی که از یک مرورگر انترنتی استفاده می کنید، ممکن است کارهایی را که انجام می دهید ضبط کند، رمز های عبور و اطلاعات مالی را ذخیره کرده و کوکی ها را از وب سایت های قبلاً بازدید شده دانلود کند. براوزنگ خصوصی به جلوگیری از برخی از این موارد کمک می کند و استفاده از آن در کمپیوتر عامه از اهمیت ویژه ای برخوردار است.

کوکی ها
کوکی ها به اطلاعاتی ارسال شده از یک مرورگر انترنت و ذخیره شده بر روی کمپیوتر شما ارتباط دارد. با این کار وب سایت ها می توانند رمزهای عبور و سابقه گردش شما را به خاطر بسپارند و ضبط کنند. اگر یک وب سایت به شما هشدار داد که از کوکی ها استفاده می کند، با استفاده از وب سایت شما به آن اجازه دسترسی به آثار فعالیت های دیجیتال خود را داده اید، که ممکن است منجر به تبلیغات هدفمند شود.



آثار فعالیت های دیجیتالی اساسی شما

کارفرمایان و صاحبان زمین ممکن است از طریق حساب رسانه اجتماعی یک کارمند یا مستاجر احتمالی جستجو کنند تا اطلاعات بیشتری در مورد آنها کسب کنند.

اگر یک کارفرما حساب توییتر، فیس بوک یا اینستاگرام شما را پیدا کند، آنها چه فکر خواهند کرد؟

برای مدیریت آثار فعالیت های دیجیتالی اساسی خود شما میتوانید دو کار را انجام دهید. نخست، تنظیمات محرمیت دلخواه خودرا در تمامی حساب های رسانه اجتماعی خود عیار کنید. دوم، **فقط چیزی را پست کنید که اگر توسط همه دیده شود برای تان مشکلی نباشد**. همیشه احتمال دارد که آنها ببینند!

مجموع آثار فعالیت های دیجیتالی شما

آثار فعالیت های دیجیتالی شما را تنها آن چیزهایکه فکر می کنید عامه ساخته شده شکل نمی دهد. شرکت ها، مجریان قانون، دولت ها و مجرمان سایبری اطلاعاتی را از کاربران اینترنت جمع می کنند. **اطلاعات شما می تواند به روش های مختلفی از ایجاد تبلیغات هدفمند تا سرقت هویت شما استفاده شود.**

در چه مواردی یک شرکت می تواند اطلاعات مربوط به آثار فعالیت های دیجیتالی شما را به مجریان قانون ارائه دهد؟ آیا این امر قانونی است؟

در حالی که برای شرکت ها مجاز است آثار فعالیت های دیجیتالی شما را به اشتراک بگذارند، برخی از شرکت ها پالیسی هایی علیه آن دارند. شما می توانید با استفاده از یک سرویس VPN ، از آثار فعالیت های دیجیتالی خود برای مخفی نگهداشتن حضور آنلاین خود، گشت و گذار در حالت براوزنگ خصوصی برای جلوگیری از کوکی ها، و با دقت کارهایی که آنلاین انجام می دهید، محافظت کنید!

بدافزارها، ویروس ها، محافظت در برابر ویروس و فایروال ها

روش های بسیاری وجود دارد که کلاهبرداران و مجرمان سایبری می توانند به اطلاعات شما دسترسی داشته باشند. پس از دسترسی به دستگاه شما، یا معلومات شخصی قابل تشخیص شما را ردیابی می کنند، می توانند خط اعتباری را به نام شما باز کنند، خرید را به حساب چک خود چارج کنند و از حساب پس انداز شما سرقت کنند. ویروس ها و بد افزارها عبارت از ابزارهای اصلی می باشند که با مجرمین در این امر یاری می رسانند. **با داشتن نرم افزار انتی ویروس و فایروال های معتبر، از دستگاه و خودتان محافظت کنید!**

اصطلاحات کلیدی

بدافزار
بدافزار هر نوع نرم افزار مخرب است که برای دستیابی یا آسیب رساندن به دستگاه الکترونیکی طراحی شده است. این اغلب برای سرقت پول طراحی شده است. ویروس های کمپیوتری نوعی نرم افزار مخرب هستند که به مجرمان سایبری امکان دسترسی به اطلاعات بانکی شما را می دهند و به کریدت (اعتبار) شما صدمه میرساند (*برای معلومات بیشتر در مورد کریدت، بررسی کنید 4.1*).

ویروس کمپیوتر
یک ویروس کمپیوتری عبارت از نرم افزار یا کد مخرب است که دارای هدف تغییر در عملکرد یک دستگاه است. ویروس ها می توانند بین دستگاههای متصل پخش شده، رمز های عبور را سرقت نموده، به سیستم وارد شده، فایلها را فاسد سازند، مخاطبین ایمیل اسپم و حتی دستگاه را تصرف کنند. آنها از طریق ضمیمه های ایمیل، فایل ها و برنامه های دانلود شده و محتویات رسانه های اجتماعی مشترک پخش شوند.

محافظت در برابر ویروس
چندین شرکت ها، مثل نورتن، نرم افزار محافظت در برابر ویروس تولید می کنند. این بسته های نرم افزاری قابل دانلود هزینه ماهانه دربر دارند، اما محافظت جدی در برابر بدافزارها و ویروس ها دارند.

فایروال
یک فایروایل مشابه نرم افزار انتی ویروس برای اتصال انترنت شما می باشد. تردد ورودی و خروجی شبکه را نظارت و مورد کنترول قرار میدهد. همچنین موانعی بین شبکه های داخلی قابل اعتماد و شبکه های خارجی غیر قابل اعتماد ایجاد می کند.

نشانی های که شما ممکن ویروس داشته باشید

- آشکار شدن دریچه های پاپ اپ طور اغلب
- تغییرات در صفحه اصلی شما
- ایمیل هایی که از حساب شما ارسال شده اند که شما ننوشته اید
- خرابی های معمول در کمپیوتر یا برنامه های شما
- عملکرد کندتر از اوسط
- برنامه های نامعلوم در دستگاه تان
- فعالیت های عجیب

چگونه از بدافزار و ویروس ها جلوگیری کرد

- روی تبلیغات پاپ اپ کلیک نکنید
- از اتصالات شبکه مصئون استفاده کنید، و صفحه کمپیوتر هایی را که محافظت از ویروس ندارند به انترنت وصل نکنید
- همیشه قبل از دانلود نمودن فایل ها آنرا سکن کنید
- از یک نرم افزار ضد ویروس با اعتبار استفاده کنید

HIAS

1.7 سوادآموزی دیجیتالی | مرور اجمالی

اطلاعات نادرست

اینترنت اطلاعات را به آسانی در دسترس قرار داده است. همچنین امکان انتشار سریع اطلاعات را فراهم ساخته است. امروز، شما می توانید به راحتی اطلاعات مربوط به رویدادهای فعلی را بصورت آنلاین یافت کنید، اما **هر آن چیزی که در اینترنت می خوانید درست نیست**. چه اطلاعات خود را از طریق رسانه های اجتماعی بدست آورید و چه از منابع خبری، همیشه باید آنچه را که آنلاین میخوانید، بررسی کنید تا صحت آن تائید شود.

خبرهای جعلی

اخبار جعلی عبارت جدیدی است که اطلاعات غلط را در سیستم عامل های رسانه های اجتماعی، مانند فیس بوک و توییتر شرح می دهد. این عبارت امروزه معمولاً توسط افراد و رسانه ها استفاده می شود. به عبارت ساده تر، اخبار جعلی بدان معنی است که این اطلاعات نادرست است و دارای هیچ گونه حقایق، منابع یا نقل قول های قابل اثبات نمی باشند. اخبار جعلی میتواند به یک اشتباه اطلاق گردد. به عنوان مثال، اگر یک منبع خبری اطلاعاتی را که بررسی نشده است به اشتراک می گذارد، که بعداً درک می کنند نادرست بوده است. اخبار جعلی همچنین می تواند اطلاعات نادرستی باشد که عمداً به اشتراک گذاشته می شود. افراد حتی ممکن است چیزی را اخبار جعلی بنامند که این میتواند واقعی باشد.

به نظر کسانی که با اینترنت ناآشنا هستند، بسیاری از منابع طنزآمیز یا طعنه آمیز، منابع رسانه ای حقیقی باشد. معلومات در پلت فرم های طنزآمیز حقیقی نمی باشند. یک پلت فرم معروف طنز عبارت از Onion است - شما می توانید این منبع را در theonion.com بخوانید.

شناسایی اطلاعات نادرست همیشه آسان نمی باشد. **همیشه از رسانه های معتبر و بی طرفانه به عنوان منبع خبر خود استفاده کنید.** می توانید برای اخبار خود از یکی از برنامه های وب مطمئن زیر بازدید کنید: New York Times, Wall Street Journal, Washington Post, National Public Radio (NPR), Economist, New Yorker, Reuters, Atlantic, or Politico.

در نهایت، منبع رسانه ای مورد نظر شما تصمیم خود شماست. همیشه سعی کنید دیدگاه های مختلف را بخوانید. به عنوان مثال، شاید منبع رسانه ای مورد نظر شما در بالا ذکر شده باشد. اگر چنین است، خواندن یک منبع خبری بین المللی، مانند BBC را نیز در نظر بگیرید. این دیدگاه ایالات متحده و بین المللی در مورد اخبار را فراهم می کند و به شما این امکان را می دهد تا نظرات خود را در مورد سیاست، دولت و سایر رویدادهای فعلی شکل دهید.

شناسایی اطلاعات نادرست

هیچ راه آسانی برای شناسایی اطلاعات نادرست وجود ندارد، اما می توانید با انجام مراحل زیر شروع کنید:

- هر آن چیزیکه میخوانید را مورد سوال قرار دهید
- درک کنید کدام پلت فرم ها معمولاً اطلاعات غلط را ارائه می دهند
- حقایق را مورد تحقیق قرار دهید

همچنین می توانید از برنامه هایی مانند بررسی واقعیت رویترز برای مشاهده اطلاعات غلط استفاده کنید: www.reuters.com/fact-check.

Infodemic

در مارچ سال 2020، سازمان صحی جهان (WHO) اطلاعات غلط موجود در اینترنت راجع به بیماری همه گیر کروناویروس را یک "infodemic" نامید. برای مقابله با اطلاعات غلط موجود در رسانه های اجتماعی، WHO کمپاین را برای دفع شایعات گسترده درمورد کورونا ویروس شروع کرد. به عنوان مثال، خوردن سیر برای محافظت افراد در برابر مصاب شدن به کرونا ویروس اثبات نشده است.

HIAS