امنیت و امنیت اینترنت

نکات ضروری برای محافظت از خود در اینترنت

امروز ما درباره موضوعی بحث خواهیم کرد که برای هر کسی که از اینترنت استفاده می کند بسیار مهم است و آن ایمنی و امنیت اینترنت است. در عصر دیجیتال امروز، ما بیش از هر زمان دیگری به هم متصل هستیم و اینترنت به بخشی جدایی ناپذیر از زندگی روزمره ما تبدیل شده است. با این حال، این افزایش اتصال با مجموعه ای از خطرات و چالش های خاص خود همراه است، از جمله حملات سایبری، سرقت هویت، کلاهبرداری های آنلاین و موارد دیگر. این خطرات می توانند عواقب جدی داشته باشند، بنابراین مهم است که از این خطرات آگاه باشیم و اقداماتی را برای محافظت از خود به صورت آنلاین انجام دهیم. در این ارائه، ما در مورد برخی از استراتژی‌های کلیدی و بهترین روش‌ها برای ایمن ماندن و ایمن ماندن آنلاین صحبت خواهیم کرد.

رمزهای عبور

هدف: درک نحوه ایجاد رمزهای عبور قوی و منحصر به فرد، و نحوه ذخیره ایمن آنها.

هر وب‌سایتی که از شما می‌خواهد حساب کاربری ایجاد کنید - بانکداری، خرید آنلاین (مانند آمازون)، رسانه‌های اجتماعی (مانند فیس‌بوک) و غیره - همچنین از شما می‌خواهد که یک رمز عبور ایجاد کنید. شما معمولاً یک نام کاربری منحصر به فرد ایجاد می کنید یا از آدرس ایمیل خود استفاده می کنید و سپس از شما خواسته می شود یک رمز عبور مخفی ایجاد کنید که فقط شما می دانید. به این ترتیب، هیچ کس دیگری نمی تواند به عنوان شما وارد سیستم شود و از حساب شما استفاده کند.

به بانکداری آنلاین فکر کنید... اگر کسی نام کاربری و رمز عبور شما را می دانست، می تواند وارد حساب شما شود و تمام پول شما را بدزدد! یا اگر شخصی به حساب آمازون شما دسترسی داشته باشد، می تواند محصولاتی را خریداری کرده و به خانه خود ارسال کند.

بنابراین بسیار مهم است که رمزهای عبور امن ایجاد کنید - که هیچ کس نمی داند و هیچ کس نتواند آنها را حدس بزند.

تعدادی نکته

1. یک رمز عبور طولانی ایجاد کنید. هر چه رمز عبور طولانی تر باشد، حدس زدن آن سخت تر است. از حداقل 12 کاراکتر استفاده کنید.

هکرها - افرادی که سعی می کنند به طور غیرقانونی به حساب های دیگران یا داده های خصوصی مشاغل دسترسی پیدا کنند - می توانند از رایانه ها برای ایجاد رمز عبور استفاده کنند. یک کامپیوتر می تواند تا 1 میلیارد رمز عبور در ثانیه را امتحان کند و حدس بزند!

اگر فقط از یک کلمه ساده استفاده کنید، مانند "افغانستان" یا "کامپیوتر" - فقط تعداد زیادی کلمه در زبان های جهان وجود دارد (خیلی کمتر از یک میلیارد!). (من فکر می کنم تعداد دقیق آن حدود 15 میلیون کلمه استهمهزبان های جهان). بنابراین یک کامپیوتر می تواند خیلی سریع آن را حدس بزند!

با این حال، اگر یک رمز عبور کاملا تصادفی به طول 8 کاراکتر ایجاد کنید، و اگر از حروف کوچک و بزرگ و همچنین اعداد استفاده می کنید (62 کاراکتر مختلف ممکن)، 218 تریلیون رمز عبور ممکن وجود دارد! (62^8) بنابراین، یک رایانه 60 ساعت طول می کشد تا رمز عبور شما را حدس بزند.

مثال:**Jf9Kt4Chain**

فقط اضافه کردن 4 کاراکتر دیگر (یک رمز عبور 12 کاراکتری) به ما 3 می دهدسکستیلیون ممکن ها. این یک میلیارد تریلیون است. به این معنی که یک کامپیوتر تا سه میلیارد روز طول می کشد تا رمز عبور شما را حدس بزند! تقریبا غیرممکن.

مثال:**S9kFtL2QvP6x**

و هرچه رمز عبور شما طولانی تر باشد، حدس زدن برای رایانه سخت تر می شود.

خوشبختانه، بیشتر وب‌سایت‌هایی که حساب‌های آنلاین دارند، قبل از قفل کردن آن‌ها از سیستم، فقط ۳ تا ۵ رمز عبور را به افراد می‌دهند. بنابراین، یک کامپیوتر واقعاً نمی تواند یک میلیارد رمز عبور وارد کند.

یک سایت سرگرم کننده برای آزمایش رمزهای عبور احتمالی که به شما می گوید چقدر قوی هستند (و چقدر طول می کشد تا رایانه آن را حدس بزند):

- https://www.security.org/how-secure-is-my-password/

2. از ترکیبی از حروف بزرگ و کوچک، اعداد و کاراکترهای خاص مانند !، @، #، $، ٪، ^، &، *، و () استفاده کنید.

درست مانند افزودن کاراکترهای بیشتر برای طولانی‌تر کردن رمزهای عبور، استفاده از کاراکترهای خاص، حدس زدن آن را پیچیده‌تر و دشوارتر می‌کند.

بسیاری از وب سایت ها هنگام ایجاد رمز عبور الزامات خاصی دارند. آنها می گویند که باید حداقل یک طول مشخص (معمولا 8 کاراکتر یا بیشتر) و ترکیبی از حروف، اعداد و کاراکترهای خاص باشد.

3. از استفاده از اطلاعات واضح مانند نام، تاریخ تولد یا شماره تلفن در رمز عبور خود اجتناب کنید.

فرض کنید من رمز عبور خود را ایجاد کردم:**"07 آوریل 1979**

این 12 کاراکتر است، از حروف، اعداد و یک کاراکتر خاص استفاده می کند. اما این هم تاریخ تولد من است. اگر کسی تاریخ تولد من را بداند، به راحتی می تواند رمز عبور من را حدس بزند. یا، هر تاریخی برای آن موضوع را می توان با رایانه حدس زد.

در مورد اسم ها هم همینطوره

"بن ایستولدحدس زدن بسیار آسان خواهد بود.

4. برای هر حساب کاربری که دارید از یک رمز عبور متفاوت استفاده کنید. به این ترتیب، اگر یک رمز عبور به خطر بیفتد، حساب های دیگر شما همچنان محافظت می شوند.

در حالت ایده آل، هر سایتی که بازدید می کنید باید رمز عبور منحصر به فرد خود را داشته باشد. فرض کنید شما دقیقاً از رمز عبور یکسانی برای هر حساب وب سایت استفاده می کنید. و سپس، یک هکر می تواند رمز عبور شما را از یک وب سایت بدون محافظت بسیار خوب بدزدد. سپس آنها می توانند از همان رمز عبور هر کجا که حساب دارید استفاده کنند.

با این حال، این اغلب یک سناریوی واقع بینانه نیست. شما باید ده ها یا حتی صدها رمز عبور مختلف را به خاطر بسپارید.

یک راه میانه خوب این است که یک رمز عبور منحصر به فرد برای چند مورد از مهم ترین حساب های خود داشته باشید: ایمیل، بانکداری و غیره. سپس از رمزهای عبور دیگر در سایت های دیگر استفاده کنید که در صورت هک شدن مشکل کمتری ایجاد می کنند.

من شخصا؟ من 6 پسورد دارم

- یکی برای ایمیل
- یکی برای بانک من
- یکی برای آمازون
- بسته به میزان اهمیت حساب، سه رمز عبور دیگر:
  - یکی برای سایت های دیگری که امنیت در آنها حیاتی است (شاید 5-10 سایت)
  - یکی برای سایت هایی که امنیت آنها مهم است (20-30 سایت)
  - یک رمز عبور دور انداخته برای سایت هایی که اگر هک شود اهمیتی نمی دهم (بیش از 40 سایت)

و سپس، به عنوان امنیت بیشتر، من چک های منظم را در اینجا انجام می دهم:https://haveibeenpwned.com/

- این جستجوی رمز عبور معکوس است. شما عبارت رمز عبور خود را وارد می کنید (نه نام کاربری یا حساب کاربری خود). و به شما اطلاع می‌دهد که در صورت نقض اطلاعات توسط هکرها به خطر افتاده است.
- بیشتر گذرواژه‌های هک شده از سوی شخصی به دست می‌آیند که فهرستی از حساب‌های کاربری و گذرواژه‌های سایت‌های آسیب‌پذیر را سرقت می‌کند.
- همچنین می‌توانید از این برای تایپ یک رمز عبور احتمالی استفاده کنید تا ببینید آیا قبلاً استفاده شده یا به سرقت رفته است یا خیر. (برای دیدن ریسک خود)

5. استفاده از مدیر رمز عبور را در نظر بگیرید که رمزهای عبور منحصر به فرد و پیچیده را برای شما تولید و ذخیره می کند.

مرورگر وب یا دستگاه تلفن همراه شما معمولاً دارای این موارد داخلی هستند. اینها نسبتاً ایمن هستند، به خصوص اگر کسی نتواند به تلفن یا رایانه شما دسترسی داشته باشد. (پس آن رمزهای عبور را واقعاً ایمن نگه دارید!)

همچنین می‌توانید نرم‌افزارهای دیگری را برای مدیریت آن دریافت کنید (مانند 1Password، BitWarden، و غیره).

6. در صورت امکان احراز هویت دو مرحله ای (2FA) را فعال کنید. این یک لایه امنیتی اضافی به حساب های شما اضافه می کند.

این یک اقدام امنیتی جدیدتر است، که در آن نه تنها از رمز عبور خود برای ورود استفاده می کنید، بلکه یک کد به عنوان پیام متنی یا ایمیل ارسال می شود. این آن را بسیار ایمن می کند! و برای وب سایت های واقعاً مهمی که باید ایمن نگه دارید، این کار به شدت توصیه می شود.

7. رمز عبور خود را مرتباً تغییر دهید، مخصوصاً برای حساب های پرخطر مانند بانک و ایمیل.

انجام این کار می تواند دردسرساز باشد، به خصوص اگر حساب های آنلاین زیادی دارید، اما برای مهم ترین سایت ها و حساب های شما، ارزش این را دارد که حداقل یک بار در سال این کار را انجام دهید.

8. از نوشتن گذرواژه‌های خود یا ذخیره آن‌ها در مکان‌هایی که به راحتی در دسترس هستند، خودداری کنید.

حتی امن ترین رمزهای عبور نیز می توانند به خطر بیفتند، اگر فهرستی را روی کاغذ پاره ای نگه دارید. مادرم همه پسوردهایش را در یک دفترچه کوچک نگه می داشت. و کتابچه ای که در کیفش نگه داشته بود. فکر می کنید چه اتفاقی افتاد که یک روز کیف او را دزدیدند؟؟؟

حریم خصوصی

هدف: یاد بگیرید چگونه از اطلاعات شخصی خود به صورت آنلاین محافظت کنید، مانند تنظیم تنظیمات حریم خصوصی در پلتفرم های رسانه های اجتماعی و اجتناب از اشتراک گذاری بیش از حد.

حریم خصوصی چیزی بیش از حفظ امنیت رمزهای عبور است. اما در مورد محافظت از اطلاعات مربوط به خود، به ویژه اطلاعات حساس یا شخصی. چیزهایی مانند:

- آدرس خانه
- شماره تلفن
- اطلاعاتی در مورد خانواده شما
- اطلاعات پزشکی
- اطلاعات مالی

اگر کسی این اطلاعات را در مورد شما پیدا کند، نمی دانید چگونه ممکن است علیه شما استفاده شود. این نوع اطلاعاتی است که هکرها می توانند سرقت کنند.

یک سناریوی بسیار واقعی: شخصی تمام نمایه فیس بوک خود را برای عموم باز کرده است. آنها یک هفته به تعطیلات می روند و شروع به ارسال تصاویر تعطیلات خود می کنند. دزدی این را می‌بیند و می‌فهمد که در خانه نیستند و سپس می‌داند که می‌توانند بدون اینکه دستگیر شوند، نفوذ کنند.

- به‌روزرسانی‌های وضعیت رسانه‌های اجتماعی نکاتی درباره سارقان، نمایش‌های مطالعاتی

از آنچه در اینترنت پست می کنید آگاه باشید! و بدانید چه کسی می تواند به روز رسانی های نمایه شما را ببیند!

گردآوری داده ها و اطلاعات

در ایالات متحده، قوانین زیادی در مورد نحوه ردیابی و ذخیره داده های مربوط به شما توسط شرکت ها وجود دارد. اما به اندازه کافی وجود ندارد!

به عنوان مثال، آیا می دانید چرا فیس بوک رایگان است؟ زیرا آنها در حال جمع آوری اطلاعات در مورد شما و فروش آن به تبلیغ کنندگان هستند. سپس آن تبلیغ‌کنندگان سعی می‌کنند محصولات را بر اساس آن اطلاعات به شما بفروشند. فیس بوک از شما درآمد کسب نمی کند، بلکه از تبلیغ کنندگانی که می خواهند همه چیز را در مورد شما بدانند، درآمد کسب می کند.

- بنابراین، ممکن است واقعاً دوست داشته باشید در Target خرید کنید. اما با دانستن تعداد فرزند و سن آنها در مورد Target چه احساسی دارید؟ یا در مورد چیزهایی که در اینترنت جستجو کردید؟ یا انواع بیماری های پزشکی که شما و خانواده تان داشته اید؟

معمول نیست که این نوع اطلاعات به دلایل بد علیه مردم استفاده شود. اما هنوز هم باعث ناراحتی بسیاری از ما می شود.

تنظیم تنظیمات

شرکت‌های رسانه‌های اجتماعی - مانند فیس‌بوک، توییتر، اینستاگرام و غیره - تنظیماتی دارند که می‌توانید آنها را پیکربندی کنید تا اطلاعات خود را خصوصی‌تر نگه دارید.

چند نمونه ازفیس بوک
- شما می توانید کنترل کنید که چه کسی مطالبی را که پست می کنید ببیند - همه و همه (توصیه نمی شود!)، فقط دوستان، فقط خودتان.
- شما می توانید کنترل کنید که چه کسی لیست دوستان شما را ببیند
- یا اینکه مردم چگونه شما را پیدا می کنند
- یا چه کسی می تواند در جدول زمانی شما پست کند
- همچنین می‌توانید پست‌های افراد دیگر را در جدول زمانی خود قبل از عمومی شدن برای تأیید/رد کردن آنها مرور کنید.

تنظیمات زیادی وجود دارد! و حتی بیشتر با در نظر گرفتن تعداد سیستم عامل های آنلاین.

فیشینگ و هرزنامه

هدف: آگاهی از نحوه شناسایی کلاهبرداری های فیشینگ و اجتناب از آنها. بدانید که با هرزنامه در صندوق ورودی ایمیل خود چه کنید.

فیشینگ از کلمه انگلیسی "fishing" گرفته شده است - اما به جای گرفتن ماهی، هکرها در تلاش برای گرفتن افراد هستند. درست مانند یک ماهیگیر که طعمه بسیار جذابی را در انتهای قلاب قرار می دهد، کلاهبرداری های فیشینگ سعی می کنند افراد را با خدمات جذاب یا مفید دستگیر کنند، اما آنها واقعاً به دنبال راهی برای دریافت پول شما هستند.

چند پیشنهاد جذاب چیست؟

1. یک مسیر سریع برای شهروندی یا وضعیت ویژه مهاجرت
2. شغلی با درآمد خوب
3. برنده شدن پول در قرعه کشی یا قرعه کشی

یک مثال

از شماره ای که در گوشی شما نیست پیامک دریافت می کنید.

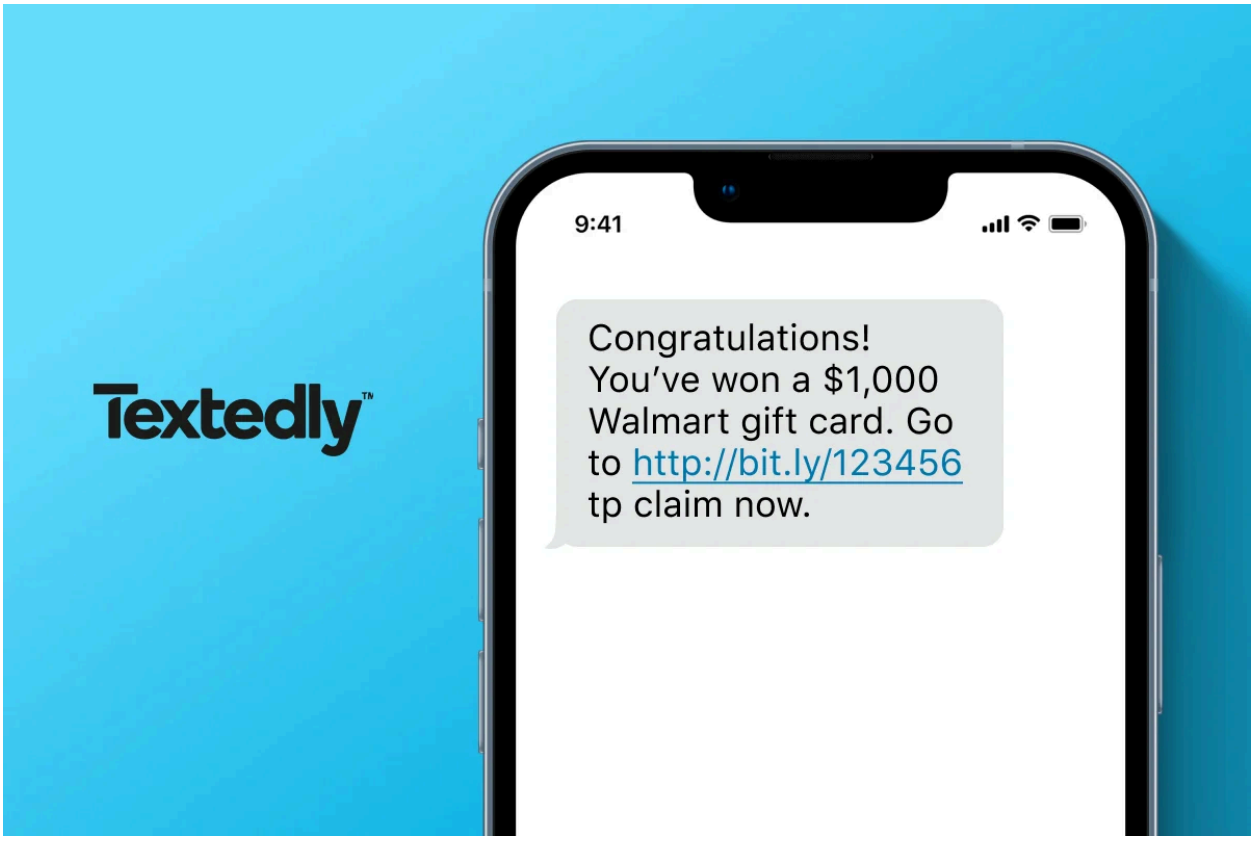
می گوید: «تبریک می گویم، شما یک کارت هدیه 1000 دلاری از Target برنده شده اید! رفتن به http://bit.ly/123456 اکنون ادعا کنیم.»

عالیه! وای!

چیزی که متوجه نمی‌شوید این است که با کلیک بر روی پیوند شما را به یک وب‌سایت جعلی هدایت می‌کند که در آن ادعا می‌کنند برای دریافت این جایزه به اطلاعات شخصی شما نیاز دارند. بنابراین شما فرم ها را پر می کنید و فرآیند را تکمیل می کنید، اما هیچ جایزه ای دریافت نمی کنید. و شما آدرس خانه، آدرس ایمیل، اطلاعات شخصی خود را داده اید... و بدترین آنها سعی می کنند شماره حساب بانکی یا سایر اطلاعات مالی را برای شما دریافت کنند.

کلاهبرداری ها به سختی کار می کنند تا این پیشنهادات بسیار واقعی به نظر برسند. گاهی اوقات تشخیص درست بودن آن سخت است.

اگر خیلی خوب به نظر می رسد که درست نباشد، معمولاً همینطور است! با شخصی که به آن اعتماد دارید، کسی که در مورد اینترنت آگاه است، تأیید کنید.



مثالی دیگر

گاهی اوقات کلاهبرداری های فیشینگ از ترس به جای پاداش برای ایجاد انگیزه استفاده می کنند.

شما یک ایمیل از شخصی دریافت می کنید که ادعا می کند یک مقام اداره مهاجرت ایالات متحده است. آنها ادعا می کنند که وضعیت مهاجرت شما در خطر است و اگر اکنون اقدام نکنید، اخراج خواهید شد. از شما خواسته می‌شود که برای پرداخت هزینه‌ها یا خدماتی که از شما محافظت می‌کند یا در فرآیند مهاجرت به شما کمک می‌کند، چند صد دلار پول تهیه کنید.

اغلب اوقات، زمانی که متوجه شوند شما به دام افتاده اید، کلاهبرداری ها بیشتر درگیر می شوند. اگر یک بار به آنها پرداخت کنید، احتمالاً دوباره به آنها پرداخت خواهید کرد. آنها ممکن است برگردند و پول بیشتری بخواهند و تا زمانی که پرداخت نکنید، شما را اذیت کنند. آنها از ترس و ارعاب استفاده می کنند تا شما را وادار کنند که پول بیشتری بدهید.

بهترین محافظت شما چیست؟ حتی مکالمه را شروع نکنید. اگر کسی که نمی‌شناسید بدون توضیح قانونی به شما پیام می‌دهد یا برایتان ایمیل می‌فرستد، فقط پیام را حذف کنید. حتی جواب نده

U.S. Citizenship and Immigration Services

U.S. CUSTOMS & BORDER PROTECTION
DEPARTMENT OF HOMELAND SECURITY
1300 Pennsylvania Ave. NW, Washington, DC 20229
WW.CBP.GOV

Case Number: IN46750K
Case Category: Act (INA) section 265 (8 U.S.C 1305)
Status: Warrant issued for background Check.

Immigrant Name:

This is to notify you that USCIS has issued a warrant for background check under Act (INA) section 265 (8 U.S.C 1305) . As per our records you failed to update your AR-11(Alien's Change of Address Card) and the same has been shared with other federal agencies-US Marshal, Justice Department and Customs and Border Protection. As per immigration law of the USA you are bound to follow all protocols and instructions of these federal agencies to perform your complete background check.

In the event of non cooperation from immigrants will lead to His/Her arrest, punishable with fine/imprisonment or removal from the USA. Any immigrants with children below 18 years of age, will be sent to foster home till the background check is not completed.

Our authorized government agency will contact for background check, however due to impact of COVID-19, Please expect some delay in our response. we encourage you to register for backgrounder check and AR-11 update at our toll free line- 18773955725

For more information please visit us at WWW.USCIS.GOV or click https://www.uscis.gov/sites/default/files/document/forms/ar-11.pdf

Kind Regards

Director General
U.S. Department of Homeland Security Citizenship and Immigration Services
Attn: Change of Address 1344 Pleasants Drive
Harrisonburg, VA 22801
www.uscis.gov

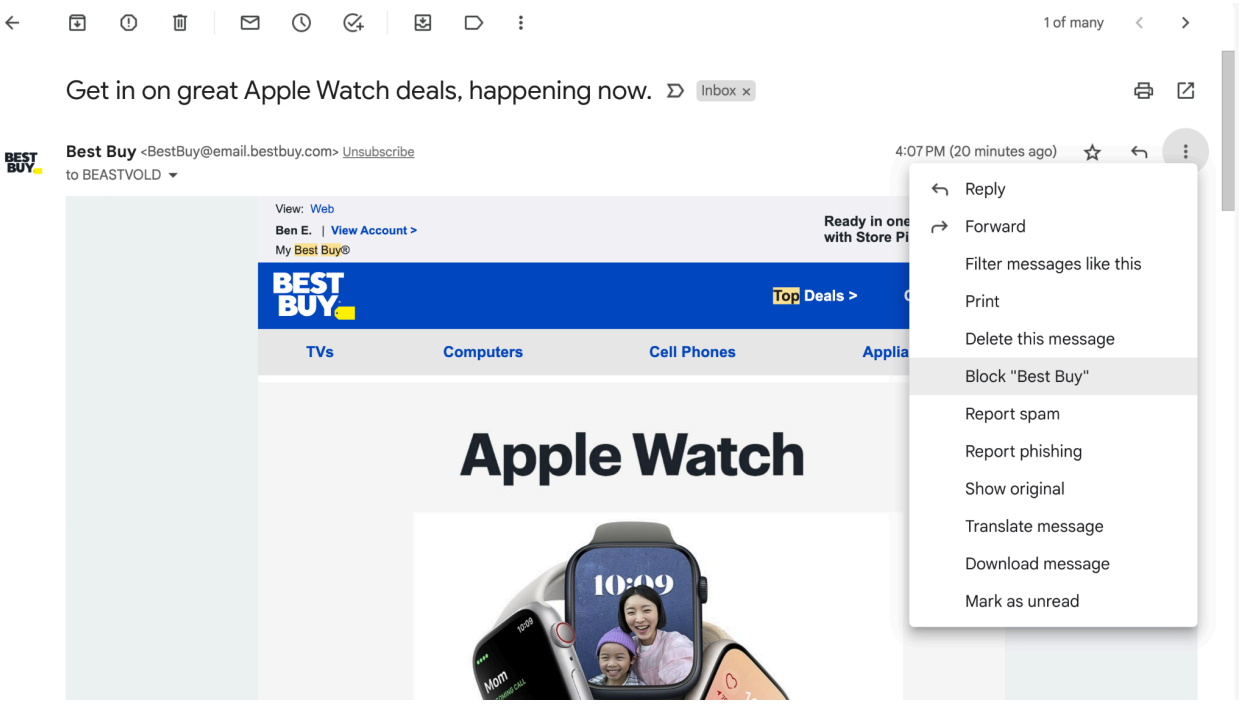
هرزنامه ها

هرزنامه چیزی است که ما به آن پیام های ناخواسته یا ناخواسته می گوییم - از طریق ایمیل یا تلفن. بیشتر اوقات، وقتی چیزی را به صورت آنلاین خریداری می کنید یا برای چیزی ثبت نام می کنید، به طور خودکار شما را در لیست ایمیل مشترک می کند. به جای تلاش برای کلاهبرداری از شما، هرزنامه معمولا سعی دارد شما را به خرید چیزی وادار کند. بیشتر اوقات، هرزنامه قانونی است - فقط آزاردهنده است. به خصوص اگر روزانه ایمیل هایی از یک کسب و کار دریافت می کنید که سعی می کند شما را به خرید یا ثبت نام چیزی وادار کند.

قانون ایالات متحده مشاغل را ملزم می کند که پیوند "لغو اشتراک" را در ایمیل های تجاری یا بازاریابی قرار دهند. بیشتر اوقات آنها در انتهای ایمیل با فونت بسیار کوچک قرار دارند. «لغو اشتراک» یا «مدیریت تنظیمات برگزیده ایمیل خود» رایج‌ترین پیوندهایی هستند که می‌بینید.

اگر اشتراک را لغو کرده‌اید و پیام‌ها همچنان ارسال می‌شوند، یا جایی برای لغو اشتراک در ایمیل نمی‌بینید، می‌توانید فقط ایمیل‌های موجود در صندوق ورودی خود را مسدود کنید.

در جیمیل، در یک ایمیل باز می‌توانید روی «سه نقطه» برای گزینه‌ها کلیک کنید. در منویی که ظاهر می‌شود، می‌توانید فرستنده را «مسدود کنید»، اگر می‌دانید در لیست پستی ثبت‌نام نکرده‌اید، «گزارش هرزنامه» یا اگر کسی قصد کلاهبرداری از شما را دارد، «گزارش فیشینگ» را انجام دهید.



ویروس ها و بدافزارها

هدف: آشنایی با انواع مختلف بدافزارها، نحوه آلوده کردن آنها به رایانه و نحوه جلوگیری و حذف آنها.

بدافزار کلمه ای است که کلمه لاتین "mal" (به معنیبد) و "ware" (مخففنرم افزار). این واقعا "نرم افزار بد" است که به شما یا رایانه شما آسیب می رساند.

انواع بدافزار

- **نرم افزارهای جاسوسی**: نرم افزاری که روی رایانه شما قرار می گیرد و از داده ها و فعالیت های شما جاسوسی می کند. اطلاعات مربوط به شما و رایانه شما به طور مخفیانه جمع آوری و برای شخص دیگری ارسال می شود - یک هکر، یک تجارت غیر اخلاقی، فروخته شده در وب تاریک و غیره.
- **ابزارهای تبلیغاتی مزاحم**: نرم افزاری که پنجره هایی را با تبلیغات باز می کند یا فعالیت اینترنتی شما را به سایتی که قصد بازدید از آن را نداشتید هدایت می کند. اساساً تبلیغات است، اما انجام آن از این طریق طبق قوانین ایالات متحده غیرقانونی است.
- **ویروس**: نرم افزار متصل به برنامه دیگری که مخفیانه اجرا می شود و روی رایانه شما نصب می شود. بسته به اینکه سازنده به دنبال چه چیزی است و هدف چه کسی است، اهداف ویروس می تواند بسیار متفاوت باشد. یک ویروس می تواند داده های شما را بدزدد، به رایانه شما آسیب برساند، از رایانه شما هرزنامه بفرستد یا ارز دیجیتال استخراج کند.

- **باج افزار**: نرم افزاری که مخفیانه روی کامپیوتر شما نصب می شود و کامپیوتر شما را خاموش می کند و از دسترسی شما به عملیات عادی جلوگیری می کند. داده‌های شما برای همیشه حذف می‌شوند مگر اینکه باج (معمولاً ارز دیجیتال) برای بازگرداندن آن‌ها پرداخت کنید.
- چندین مورد دیگر: کرم ها، بات نت ها، تروجان ها، روت کیت ها و غیره.



بهترین راه برای محافظت از خود

1. **به وب سایت هایی که نمی شناسید یا به آنها اعتماد ندارید مراجعه نکنید**. تنها با بازدید از یک وب سایت مخرب می توانید ویروس ها را دانلود و بر روی رایانه خود نصب کنید. اگر مطمئن نیستید، می توانید سایت را با استفاده از وضعیت سایت مرور ایمن Google بررسی کنید:
   a. https://transparencyreport.google.com/safe-browsing/search
2. **روی پیوندهایی که نمی شناسید کلیک نکنید** از پیامک یا ایمیل گاهی اوقات با قرار دادن نام یا غلط املایی در پیوند وانمود می کنند که تجارت قانونی هستند:
   a. https://www.weiisfarg0.com (به "i" به جای "l" و "0" به جای "o" توجه کنید.
   b. https://bank-info.biz/wellsfargo.com (آنها فکر می کنند که فقط قرار دادن نام قانونی در URL شما را فریب می دهد تا روی آن کلیک کنید.
3. **از آنتی ویروس خوب محافظت کنید** برای کامپیوتر شما گزینه های رایگان مناسبی وجود دارد:
   a. AVG، Avast، BitDefender، Avira
   b. https://www.pcmag.com/picks/the-best-free-antivirus-protection

4. **در مورد باز کردن هر نوع پیوست ایمیل بسیار محتاط باشید** که انتظارش را ندارید، به خصوص اگر از طرف کسی باشد که نمی‌شناسید.
    a. ویروس ها را می توان به اسناد Word، فایل های فشرده، فایل های اجرایی و غیره متصل کرد.
5. **سیستم عامل خود را به روز نگه دارید** (ویندوز، سیستم عامل مک، iOS، سیستم عامل اندروید). این کسب‌وکارهای بزرگ به ارائه محصولات ایمن اختصاص یافته‌اند، بنابراین دائماً با رفع اشکال و امنیت بیشتر به‌روزرسانی می‌شوند.
6. **در هات اسپات های وای فای عمومی مراقب باشید**. اگر بتوانید بدون محافظت پیشگیرانه به راحتی به اینترنت دسترسی داشته باشید، به این معنی است که شخص دیگری با نیت بد نیز می تواند این کار را انجام دهد. با قرار گرفتن در یک شبکه، آنها می توانند با نظارت بر ترافیک شما یا دسترسی به منابع رایانه شما، سعی کنند از راه دور رایانه شما را هک کنند.
    a. [آیا تلفن شما در برابر مهاجمان سایبری فرودگاه آسیب پذیر است؟]
    b. بهترین راه برای ایمن ماندن؟
        i. متصل نشوید؛ فقط از اپراتور تلفن همراه خود به عنوان نقطه اتصال خود استفاده کنید.
        ii. یا، اگر آنتی ویروس و نرم افزار سپر وب خوبی دارید، که می تواند از بسیاری از تهدیدات محافظت کند
        iii. (پیشرفته تر) یک اتصال رمزگذاری شده شبکه خصوصی مجازی (VPN) از هرگونه چشم جاسوسی در برابر فعالیت شما محافظت می کند.

ایمن نگه داشتن کودکان

ممکن است در اینترنت احساس راحتی کنید و خود را ایمن نگه دارید - اما در مورد فرزندانتان چطور؟ آنها به احتمال زیاد خود را به دردسر می اندازند یا به محتوایی که نباید دسترسی پیدا کنند.

دسترسی به اینترنت و زمان را محدود کنید

دستگاه‌های تلفن همراه مانند آیفون و تلفن‌های هوشمند اندرویدی گزینه‌هایی برای محدود کردن زمان نمایش برای کودکان تعبیه کرده‌اند. شما می توانید برنامه هفتگی، روزها و ساعاتی را که آنها می توانند به آن دسترسی داشته باشند را کنترل کنید. همچنین می‌توانید روی سایت‌ها و برنامه‌هایی که بازدید می‌کنند کنترل داشته باشید.

اندروید:https://support.google.com/families/answer/7103340?hl=fa

iPhone/iPad:https://support.apple.com/en-us/HT208982

همچنین نرم افزاری وجود دارد که می توانید برای کنترل بیشتر روی رایانه ها نصب کنید:

- بهترین نرم افزار کنترل والدین برای سال 2023

فعالیت آنها را زیر نظر داشته باشید

کودکان باید بدانند که شما می توانید در هر زمان به دستگاه های آنها دسترسی داشته باشید. می‌توانید ایمیل، رسانه‌های اجتماعی، پیام‌ها و تاریخچه مرور اینترنت آنها را بررسی کنید.

بزرگسالان جوان می توانند در پنهان کردن استفاده خود بسیار ماهر باشند - حذف سابقه مرور، ایجاد حساب های رسانه های اجتماعی جعلی و غیره. هیچ راه احمقانه ای برای محافظت در برابر هر نگرانی وجود ندارد. در عوض، آموزش مسئولیت‌پذیری و مسئولیت‌پذیری را تمرین کنید، بنابراین به گفتگو با فرزندان خود در مورد نحوه استفاده از دستگاه‌ها ادامه می‌دهید.

از وب سایت های امن استفاده کنید

محتوای زیادی در YouTube وجود دارد که نمی‌خواهم فرزندانم ببینند. خوشبختانه وجود دارد YouTube Kids جایی که من نسبت به آنچه که آنها می بینند و تماشا می کنند احساس راحتی بیشتری می کنم.

KidsSearch.com موتور جستجویی است که از جستجوی ایمن گوگل و فیلتر کردن آن برای محدود کردن آنچه کودکان در اینترنت پیدا می‌کنند استفاده می‌کند.

فقط در فضاهای عمومی خانه استفاده شود

اگر نگران نحوه استفاده فرزندانتان از وسایل هستید، اجازه ندهید آنها در اتاق خود یا پشت درهای بسته از آنها استفاده کنند.

برای فرزندان خود من (۹ و ۱۱ ساله)، هنگام استفاده از دستگاه‌هایشان (حتی Chromebook مدرسه) باید درهای اتاق خوابشان را باز نگه دارند. و آنها اجازه ندارند دستگاه های خود را در اتاق خود در شب نگه دارند. (آنها را در اتاق ما می گذارند.)

با فرزندان خود در مورد امنیت اینترنت صحبت کنید

همه چیزهایی که در اینجا در مورد آنها صحبت می کنیم - با بچه های خود صحبت کنید! باور کنید آنها به سرعت این مطالب را یاد خواهند گرفت.