SANS SECURITY AWARENESS

ماهنامه آگاهی از امنیت اطلاعات برای شما

آیا هک شدم؟

مقدمه

مهم نیست تا چه حد امنیت دارید، درست مانند رانندگی ماشین دیر یا زود ممکن است تصادف کنید. در ذیل به نکاتی می پردازیم که به شما کمک خواهد کرد تا تشخیص دهید آیا هک شده اید یا خیر و در صورت هک شدن چه اقداماتی باید انجام دهید. چنانچه هر چه سریعتر درباره چیز بدی که اتفاق افتاده مطلع شوید، احتمال بیشتری وجود خواهد داشت که آن مشکل را برطرف سازید.

سرنخ هایی که نشان میدهد هک شده اید

برنامه ویروس یاب شما هشداری را ایجاد میکند که نشان میدهد سیستم شما آلوده شده است. مطمئن شوید که این هشدار واقعا توسط برنامه ویروس یاب صادر شده و یک پنجره پاپ آپ از یک سایت مخرب نیست که از شما بخواهد با یک شماره تماس بگیرید و یا یک برنامه دیگری را نصب کنید. اگر مطمئن نیستید برنامه ویروس یاب خود را باز کنید.

یک پنجره پاپ آپ بر روی سیستم شما طاهر میشود و به شما پیغام میدهد که دستگاه شما رمزگزاری شده و باید به باجگیر مبلغی پرداخت کنید تا فایلهای خود را پس بگیرید.

مرورگر شما از شما میخواهد به انواع وب سایت هایی بروید که شما تمایلی به رفتن با آن وب سایت ها ندارید.

کامپیوتر و یا برنامه های شما دائما در حال کرش کردن و خارج شدن از عملکرد طبیعی هستند، آیکون هایی از برنامه های ناشناخته بر روی سیستم وجود دارد یا پنجره های عجیب در کامپیوتر شما باز میشوند.

رمز عبور شما دیگر کار نمیکند با اینکه از درستی آن مطمئن هستید

دوستان شما از شما می پرسند که چرا برای آنها هرزنامه میفرستید درحالیکه شما اطمینان دارید برای آنها ایمیلی نفرستادید.

از حساب بانکی شما مبالغی دریافت شده و یا صورت حسابی پرداخت شده که شما هرگز آن را انجام ندادید.

چگونه پاسخ بدهیم

اگر مشکوک هستید که سیستم شما هک شده است، بهتر است هرچه زودتر دست به کار شوید. اگر هک شدن با کار شما در ارتباط است، سعی نکنید خودتان مشکل را برطرف کنید، بجای این کار بلافاصله گزارش دهید. اگر سیستم و یا حساب شخصی شما هک شد، در ذیل قدمهایی که میتوانید بردارید را ذکر میکنیم.

رمز عبور خود را تغییر دهید: این کار نه تنها شامل تعییر رمز عبور کامپیوتر و موبایل شما میشود، بلکه لازم است رمز عبور حساب های آنلاین خود را نیز تغییر دهید. از کامپیوتری که هک شده برای تغییر رمز عبور استفاده نکنید، از دستگاهی استفاده کنید که به امن بودن آن اطمینان دارید. اگر حساب کاربری زیادی دارید از مهمترین آنها شروع کنید. اگر نمیتوانید تمامی رمز عبور های خود را بخاطر بسپارید، از برنامه های مدیریت رمز عبور استفاده کنید.

مالی: در مواجهه با مشکلاتی که برای کارت اعتباری و یا حسابهای مالی شما رخ میدهد، بلافاصله با بانک و یا شرکت کارت اعتباری خود تماس بگیرید. به یک شماره تماس قابل اعتماد، نظیر آنچه در پشت کارت اعتباری شما نوشته شده تماس بگیرید و یا توسط یک کامپیوتر مطمئن به وب سایت آنها مراجعه کنید. علاوه بر این میتوانید از شرکت سرویس دهنده بخواهید اطلاعات مالی شما را به اشتراک نگذارند و حساب شما را ببندند(Credit freeze) .

ویروس یاب: اگر برنامه ویروس یاب به شما درباره فایلی آلوده اطلاع میدهد، اقدامات توصیه شده توسط برنامه ویروس یاب را دنبال کنید. اغلب برنامه های ویروس یاب حاوی لینک هایی هستند که توسط آن قادر خواهید بود تا درباره آلودگی خاص اطلاعات بدست آورید.

نصب مجدد: اگر نمیتوانید کامپیوتر آلوده را درست کنید یا میخواهید از امنیت دستگاه خود مطمئن باشید، سیستم عامل آن را مجدد نصب کنید. از فایلهای پشتیبان برای نصب مجدد استفاده نکنید، از آن فقط برای بازیابی فایلهای شخصی خود استفاده کنید. اگر قادر به این کار نیستید، از افراد خبره بخواهید به شما کمک کنند. اگر کامپیوتر و یا دستگاه شما قدیمی است، بهتر است مدل جدید آن را خریداری کنید. در خاتمه اگر سیستم خود را مجددا نصب کردید و یا مدل جدیدتری خریدید، اطمینان حاصل کنید که بروزرسانی شده باشد و با فعال کردن بروزرسانی خودکار تمامی سیستم بصورت اتوماتیک بروزرسانی شود.

پشتیبان ها: قدم کلیدی برای محافظت از خودتان این است که قبل از هر اتفاق از سیستم خود بصورت منظم پشتیان گیری کنید. راه حل های زیادی وجود دارد تا از سیستم خود بصورت روزانه و یا ساعتی پشتیبان بگیرید. صرف نظر از اینکه از چه راهکاری برای پشتیان گیری منظم استفاده میکنید، چک کنید که فایلها قابل بازیابی هستند. بسیاری از اوقات تنها راه بازیابی سیستمی که هک شده استفاده از فایلهای پشتیبان است.

اجرای قانون: اگر به هر دلیلی احساس کردید که تهدید شده اید، حادثه را به مجری قانون گزارش کنید. اگر در آمریکا قربانی سرقت هویت شدید میتوانید از این لینک https://www.identitytheft.gov استفاده کنید.

سردبیر مهمان

دکتر یوهانس اولریش (@johullrich) معاون تحقیق در موسسه تکنولوژی SANS، مدیر مرکز طوفان اینترنتی و یکی از اعضای SANS است. وی سازنده شبکه حسگر به نام DShield بوده و بصورت روزانه میهمان مرکز طوفان اینترنتی است و اخبار امنیت شبکه را به شکل پادکست ارائه می دهد.

منابع

پشتیبان ها: https://www.sans.org/u/JGP
کلمات عبور: https://www.sans.org/u/JGU
مدیریت رمزعبور: https://www.sans.org/u/JGZ
بدافزار چیست: https://www.sans.org/u/JH4
بستن اعتبار: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/