وای! ژ ا نویه 2020

SANS SECURITY AWARENESS

OUCH!

ماهنامه آگاهی از امنیت اطلاعات برای شما

وراثت دیجیتالی

مقدمه

آیا تا به حال در مورد این سوال دشوار فکر کرده اید که «چه اتفاق برای حضور دیجیتالی ما می افتد وقتی که می میریم یا ناتوان از دسترسی به اینترنت می شویم؟» بسیاری از ما یا قبلا وصیت نامه خود را تنظیم کرده ایم یا می دانیم که باید فهرستی از آنچه عزیزان باید بدانند داشته باشیم. اما در مورد همه داده های دیجیتال و حساب های آنلاین چه برنامه ای داریم؟ آیا باید در فکر تنظیم نوعی وصیت نامه دیجیتال باشیم؟ آیا ما باید برنامه ای برای «وراثت دیجیتال» داشته باشیم؟

به حضور دیجیتالی خود بیاندیشید. حساب های بانکی و بازنشستگی، وام مسکن، عکس و فیلم های خانوادگی، حساب های کاربری کنترل خانه هوشمند، ایمیل و رسانه های اجتماعی فقط برخی از نمونه های زیادی هستند که ردپای دیجیتالی ما را تشکیل می دهند. در صورت فوت شما یا عضو نزدیکی از خانواده، ممکن است خانواده و عزیزان به دسترسی سریع به آن حساب یا داده ها نیاز داشته باشند. علاوه بر این، داده های قدیمی و حساب های آنلاین باقی مانده می توانند با گذشت زمان برای هکرها مفید واقع شوند، و اینگونه خانواده و دوستان مرحوم را در معرض خطر قرار دهند.

برنامه ریزی کنید

این ایده خوبی است که مانند سایر جزئیات که در پایان زندگی به آنها فکر میکنیم، در مورد خواسته های خود با خانواده یا دوستان قابل اعتماد خود صحبت کنید. علاوه بر داشتن این مکالمات، دارایی های دیجیتالی و حساب های آنلاین خود را نیز جمع آوری و مستند کنید. اگر بعد از مردن دسترسی به حسابهای خود فراهم نکنید، دسترسی یا بستن آنها توسط اعضای خانواده ممکن است بسیار دشوار باشد. به عنوان مثال، آیا می خواهید اعضای خانواده شما از تمام عکس های خانوادگی و فیلم هایی که در اینترنت ذخیره کرده اید، بخاطر نداشتن دسترسی محروم شوند؟

یک ایده این است که گذرواژه های خود را در یک نرم افزار مدیریت گذرواژه ثبت کنید. اینها برنامه هایی هستند که به طور ایمن تمام گذرواژه های شما، کارت های اعتباری و سایر اطلاعات حساس را ذخیره می کنند. طوری طراحی شده اند که ایجاد، ذخیره و دسترسی به گذرواژه‌ها و سؤالات امنیتی بسیار ساده شوند. از بسیاری جهات، اینها ابزاری قدرتمند برای فهرست کردن حضور دیجیتالی شماست. بسیاری از این نرم افزارهای مدیریت گذرواژه اجازه به اشتراک گذاشتن بعضی یا همه گذرواژه ها با سایر اعضای خانواده را میدهند. اگر با این کار راحت نیستید، نحوه دسترسی به نرم افزار مدیریت گذرواژه ها را ثبت کنید و آن را در یک پاکت نامه گذاشته مهر و موم کنید.

و از نزدیکانتان بخواهید که پس از درگذشت توسط مجری یا یکی از اعضای خانواده قابل اعتماد، آن پاکت مهر و موم شده باز شود. به این ترتیب، آنها به مدیریت گذرواژه های شما دسترسی خواهند داشت و می توانند به حساب ها و اطلاعات ذخیره شده در آنجا دسترسی داشته باشند

علاوه بر این، برخی سایت ها گزینه انتخاب و معرفی مخاطبین مورد اعتماد را ارائه می دهند. به عنوان مثال، فیس بوک اجازه می دهد تا کاربران از قبل تعیین کنند که آیا دوست دارند حسابشان بعد از گذشت حذف شده یا صفحه یادبود برایشان ایجاد شود. صفحه یادبود فضایی را ایجاد می کند که فقط برای دوستان موجود قابل مشاهده باشد، و جایی است که دوستان می توانند خاطرات خود را در مورد دوست فوت شده به اشتراک گذارند. سرانجام، شما ممکن است بخواهید که با یک وکیل یا برنامه ریز متخصص دارایی ها دیجیتال قرارداد ببندید.

به ارث بردن دارایی های دیجیتال

ممکن است در شرایطی قرار بگیرید که مجبور به بازیابی یا دسترسی به حساب های آنلاین یک دوست یا عضو خانواده که اخیرا درگذشته باشید. توصیه می کنیم قبل از اقدام، ابتدا با یک وکیل و سایر اعضای خانواده هماهنگ کنید. دیگر اعضای خانواده ممکن است خیلی ناراحت شوند، اگر ببینند که بدون هیچ مشورت با آنها شما سرخود اقدام کرده اید. سپس به شناسایی رمزهای عبور دیگری که می توانید پیدا کنید بپردازید. آیا مرحوم آنها را جایی نوشته یا ذخیره کرده؟ اگر این کار انجام نشده، آیا می توانید به هر رایانه یا دستگاه تلفن همراه که مرحوم استفاده میکرده دسترسی پیدا کنید و هنوز وارد سیستم شوید؟ اگر اینطور نیست، به احتمال زیاد باید با سایتهایی که مرحوم عضو بوده تماس بگیرید. این اغلب شامل ارائه گواهی فوت و اثبات ارتباط مستقیم با اعضای خانواده مرحوم است. در بعضی موارد، شما قادر به دسترسی به حساب یا داده های ذخیره شده در حساب نخواهید بود بلکه فقط میتوانید آن را حذف کنید. هر سایتی سیاستهای متفاوتی در این موارد دارد، که می تواند یک فرایند وقت گیر باشد.

در دنیای دیجیتال امروز، ما نباید فقط به فکر دارایی های فیزیکی خود باشیم بلکه دارایی های دیجیتال را نیز در برنامه ریزی دارایی های خود در نظر بگیریم.

سردبیر مهمان

Cheryl Conley یک کارشناس خبره در زمینه فیشینگ و آگاهی رسانی در این زمینه است که تجربه او شامل کمک به ساخت و مدیریت برنامه فیشینگ در شرکت لاکهید مارتین است. او حالا با گروه آگاهی رسانی امنیت اطلاعات SANS همکاری میکند و دارنده گواهینامه SSAP (SANS Security Awareness Professional) است.

منابع

مدیریت گذرواژه ها http://www.sans.org/u/Y5Y

آسان سازی گذرواژه ها http://www.sans.org/u/Y63