من هک شدم،چه باید کرد؟

آیا هک شده ام؟

اینترنت می تواند با فناوری های جدیدی که همیشه در حال تغییر هستند طاقت فرسا باشد. مهم نیست چقدر سعی می کنید ایمن باشید، دیر یا زود ممکن است به اندازه کافی بدشانس بوده که هک شوید. هرچه زودتر تشخیص دهید که اتفاق بدی افتاده است و هرچه سریعتر پاسخ دهید، بیشتر می توانید تأثیرهای آسیبها را به حداقل برسانید. در زیر نشانه هایی وجود دارد که نشان می دهد ممکن است شما هک شده باشید و اگر چنین است، پیشنهاداتی برای رفع آن وجود دارد.

سرنخ هایی که نشان میدهد ممکن است یکی از حساب های آنلاین شما هک شده باشد

- فامیل یا دوستانتان به شما میگویند پیغامها یا دعوت نامه های عجیبی از طرف شما دریافت میکنند، درصورتیکه شما میدانید آنها را ارسال نکرده اید.
- پسورد یکی ازاکانتهای شما دیگر کار نمیکند، اگرچه میدانید که پسوردتان را درست وارد کرده اید.
- اخطارهایی از سایتهای مختلف دریافت میکنید با این مضمون که یک نفر به اکانت شما وارد شده است، درصورتیکه میدانید خودتان وارد نشده اید.
- ایمیل هایی دریافت می کنید که تغییراتی را در پروفایل آنلاین خود تأیید کرده اید که شما آن را انجام نداده اید.

سرنخهایی که نشان میدهد کامپیوتر یا دستگاه همراه شما هک شده است

- برنامه آنتی ویروس شما هشدار میدهد که سیستمتان آلوده شده است. مطمئن شوید که این هشدارواقعا از آنتی ویروس شما تولید شده و احیانا از یک پنجره بازشو خودکار (pop-up) از یک وب سایت مخرب نیست که سعی دارد با فریب، شما را وادار به انجام تماس و یا نصب یک برنامه دیگر کند. مطمئن نیستید ؟ برنامه آنتی ویروس خود را باز کنید تا اطمینان حاصل کنید که آیا واقعا کامپیوتر شما آلوده شده است یا خیر.
- هنگام جستجو در صفحات وب، شما اغلب به صفحه هایی هدایت می شوید که نمی خواستید از آنها بازدید کنید و یا صفحات جدید و ناخواسته ظاهر می شوند.
- یک پنجره بازشو دریافت می کنید که می گوید کامپیوتر شما رمزگذاری شده است و برای بازگرداندن پرونده های خود باید باج بپردازید.

سرنخ هایی که نشان میدهد کارت اعتباری یا مالی شما هک شده است

- هزینه های مشکوک یا ناشناخته ای از کارت اعتباری شما وجود دارد یا نقل و انتقالات غیرمجاز در حساب بانکی شما هست که می دانید انجام نداده اید.

چه باید کرد؟ - چگونه کنترل رامجددا پس بگیریم

اگر شک دارید که هک شده اید، آرام باشید. شما از پس آن بر می آیید. اگر هک مربوط به کار است، سعی نکنید خودتان مشکل را برطرف کنید. در عوض، فوراً آن را گزارش دهید. اگر سیستم یا حساب شخصی شما هک شده است، در اینجا چند مرحله وجود دارد که میتوانید انجام دهید:

- بازیابی حسابهای آنلاین خود: اگر هنوز به حساب خود دسترسی دارید، از یک رایانه قابل اعتماد وارد شوید و رمز عبور خود را با یک رمز عبور جدید، منحصر به فرد و قوی بازنشانی کنید - هر چه طولانی تر، بهتر. اگر احراز هویت چند عاملی (MFA) را فعال نکرده اید، اکنون زمان خوبی برای فعال کردن آن است. اگر دیگر به حساب خود دسترسی ندارید، با وبسایت مربوطه تماس بگیرید و به آنها اطلاع دهید که حساب شما تصاحب شده است. اگر اکانت دیگری دارید که رمز عبور یکسانی با حساب هک شده شما دارد، بلافاصله آن رمزهای عبور را نیز تغییر دهید.
- بازیابی کامپیوتر یا دستگاه شخصی شما: اگر برنامه آنتی ویروس شما قادر به تعمیر کامپیوتر آلوده نیست و یا اگر میخواهید از ایمن بودن سیستم خود اطمینان بیشتری حاصل کنید، نصب مجدد سیستم عامل و بازسازی کامپیوتر را در نظر بگیرید. اگر حس خوبی نسبت به بازسازی مجدد آن ندارید یا اگر کامپیوتر و یا دستگاه شما قدیمی است، ممکن است زمان خرید دستگاه جدید فرا رسیده باشد.
- اثرات مالی: برای مشکلات کارت اعتباری یا هرگونه حساب مالی، بلافاصله با بانک یا شرکت کارت اعتباری خود تماس بگیرید. هرچه زودتر با آنها تماس بگیرید، احتمال بیشتری وجود دارد که بتوانید پول خود را بازپس بگیرید. با استفاده از شماره تلفن موجود در ایمیل با آنها تماس نگیرید، بلکه از یک شماره تلفن قابل اعتماد استفاده کنید، مانند شماره ای که در پشت کارت بانکی یا وب سایت آنها درج شده است. صورت وضعیت و گزارشات مالی و اعتباری خود را مرتب کنترل کنید. در صورت امکان، هر زمان که هزینه یا انتقال پول وجود دارد، اعلان‌های خودکار را فعال کنید.

برای جلوتر بودن از مهاجمان سایبری چه باید کرد؟

خبرنامه OUCH Security Awareness به صورت ماهانه منتشر می شود و مجموعه ای کامل در مورد چگونگی ایمن سازی خود دارد. در بخش منابع زیر، مهم‌ترین خبرنامه‌های OUCH را که باید برای محافظت از خود بخوانید، فهرست می‌کنیم. این منابع بر سه مرحله کلیدی تمرکز دارند:

1. همه سیستم‌ها و دستگاه‌های خود را به‌روزرسانی کرده و به آخرین نسخه و به‌روز نگه دارید.
2. از رمزهای عبور قوی و منحصر به فرد برای هر یک از حساب های خود استفاده کنید، آن حساب ها را با یک Password Manager مدیریت کنید و MFA را فعال کنید.
3. شک داشته باشید - مراقب تاکتیک های مهندسی اجتماعی مانند ایمیل های فیشینگ باشید.

سردبیر مهمان

سارا مورالز (@SarahManley) یک مدیر ارشد برنامه در تیم حریم خصوصی، ایمنی و امنیت Google است. او تعامل خارجی را با تمرکز بر ایجاد جامعه، همکاری و مشارکت رهبری می کند. او عضو هیئت مدیره Wicys است و فعالانه در راهکارهای DEI درون جامعه امنیت سایبری مشارکت دارد.

منابع

برنامه های مدیریت رمز عبور: https://www.sans.org/newsletters/ouch/password-managers
احراز هویت چند عاملی:یک قدم ساده برای امن کردن حسابهای شما: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts
محرکهای احساسی: چگونه مهاجمان سایبری شما را فریب میدهند: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you
حملات فیشینگ فریبکارانه تر میشوند: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier

ترجمه شده برای عموم توسط: هومن خجاو، مجید هدایتی