علاج بعد از وقوع حادثه

چه باید کرد اگر اطلاعات محرمانه ما افشا شود

همه روزه اخباری در مورد سوء استفاده از داده‌های کاربران به گوش می‌رسد. حتی شرکت‌های بزرگی که داده‌های بسیار حساس مانند جزئیات کارت اعتباری شما را نگهداری می‌کنند نیز آسیب پذیر هستند. متاسفانه امنیت سایبری این شرکت‌ها خارج از کنترل شما است. اما اگر بنا به هر دلیلی داده‌های حساس شما لو رفت، برای به حداقل رساندن خسارت اقداماتی را باید انجام دهید.

ببینید چه اطلاعاتی لو رفته است

اگر بنا به هر دلیلی داده‌های محرمانه شما درز پیدا کرد و این احتمال وجود داشت که از آن سوء استفاده شود، اولین کاری که باید انجام دهید این است که ببینید چه اطلاعاتی درز پیدا کرده است و چه خساراتی می‌تواند برای شما به همراه داشته باشد. آیا این اطلاعات مربوط به نام کاربری و کلمات عبور شما است؟ آیا این داده‌ها کدگذاری شده بودند و یا به صورت یک فایل متنی ساده ذخیره شده بودند؟ آیا اطلاعات شخصی دیگری از شما مثل تاریخ تولد، آدرس، شماره تلفن و یا حتی پاسخ‌های سوالات امنیتی شما نیز لو رفته است؟ آیا این شرکت اطلاعات پرداخت، کارت اعتباری و یا حتی شماره پاسپورت شما را نیز ذخیره کرده است؟

ببینید این رخنه چگونه صورت گرفته است. آیا اولین بار قبل از این که توسط دیگران دیده شود، توسط توسعه دهندگان داخلی شرکت خسارت دیده کشف شده است؟ و یا این که بعد از سرقت در وب تاریک فروخته شده است؟ برای یافتن پاسخ این سوالات می‌توانید با خود شرکت تماس بگیرید، اخبار را دنبال کنید و یا موضوع را جستجو کنید.

بر اساس نوع داده‌های درز پیدا کرده و نحوه انجام این کار، مراحل زیر را دنبال کنید:

اگر اطلاعات مربوط به حساب کاربری و کلمات عبور بود

اگر داده‌های لو رفته شامل ایمیل، نام کاربری، کلمه عبور، تاریخ تولد، آدرس یا اطلاعاتی شبیه به این بود، اقدامات احتیاطی زیر را انجام دهید:

1. کلمات عبور خود را فورا تغییر دهید. و حتما یک کلمه عبور سخت و طولانی به همراه ترکیبی از حروف کوچک و بزرگ، عدد و کاراکترهای ویژه انتخاب کنید.
2. برای این که ببینید کلمات عبور انتخابی شما تا چه اندازه پیچیده و غیرقابل شناسایی است می‌توانید از یک ابزار سنجش آنلاین استفاده کنید.
3. اگر از یک کلمه عبور یکسان برای چند حساب و پلتفرم مختلف استفاده می‌کنید (که هرگز نباید چنین کاری انجام دهید) آنها را نیز تغییر دهید.
4. از سیستم احراز هویت دو مرحله‌ای استفاده کنید. این به معنای آن است که اگر شخصی بنا به هر دلیلی به

کلمه عبور شما دسترسی پیدا کرد، قادر نخواهد بود به حساب کاربری شما دسترسی پیدا کند. چرا که برای ورود به یک کد دوم نیز نیاز خواهد بود که معمولا به شماره موبایل شما ارسال می‌شود و هکرها نیاز به دسترسی فیزیکی به آن دارند.

5. در مورد فیشینگ و حملات مهندسی اجتماعی مشابه اطلاعات کسب کنید. هکرها و کلاهبرداران در ابتدای امر اطلاعات کافی برای نفوذ به حساب‌های کاربری شما ندارند، اما می‌توانند از تاریخ تولد یا آدرس شما برای کلاهبرداری از شما یا خدماتی که استفاده می‌کنید بهره بگیرند. آنها ممکن است سعی کنند از این داده‌ها استفاده کنند تا شما را متقاعد کنند که از یک شرکت معتبر و قانونی هستند و با جلب اعتماد اطلاعات حساس دیگری را نیز از شما دریافت می‌کنند. مراقب باشید به دام آنها نیفتید.

اگر داده‌های لو رفته مربوط به مراقبت‌های بهداشتی بود

1. به بیمه سلامت خود اطلاع دهید که داده‌های سلامت شما درز پیدا کرده است و ممکن است شخص دیگری سعی کند از آن استفاده کند. از آنها بخواهید که هوشیار باشند و سوابق را قبل از صدور هرگونه پرداخت بررسی کنند.
2. سوابق پزشکی خود را بررسی کنید و در مواردی که شخصی قبلا سعی داشته تحت نام شما ادعایی داشته باشد، پرداخت‌های مربوط به بیمه سلامت را نیز بررسی کنید.

اگر اطلاعات لو رفته مربوط به حساب‌های بانکی شما است

1. با بانک خود تماس بگیرید تا کارت شما را مسدود کنند. این کار تضمین می‌کند که دیگر هیچ کس قادر به دسترسی به گزارش‌های اعتباری شما بدون اجازه شما نخواهد بود. همچنین می‌توانید حساب خود را ببندید و از بانک بخواهید کارت جدیدی برای شما صادر کند.
2. تبادلات اخیر کارت اعتباری خود را برای هرگونه فعالیت مشکوک بررسی کنید.
3. گزارش اعتباری دریافت کنید تا ببینید که آیا قبلا حساب‌های جعلی یا کارت‌های اعتباری به نام شما افتتاح یا گرفته شده است.
4. این بار نیز در مورد حملات فیشینگ اطلاعات کسب کنید. هکرها ممکن است از جزئیات اطلاعات پرداخت شما استفاده کنند و با اعلام این اطلاعات به شما از طریق ایمیل یا تماس تلفنی این‌گونه وانمود کنند که از یک شرکت قانونی هستند. چنین فریب خوردن‌هایی خیلی ساده اتفاق می‌افتد، چرا که شما تصور می‌کنید تنها شرکت‌هایی که شما به آنها اطمینان دارید می‌توانند این اطلاعات را در اختیار داشته باشند. هیچ اطلاعات دیگری در اختیار آنها قرار ندهید و یا روی لینک‌های مشکوک کلیک نکنید.

آخرین توصیه

اکنون شما برای محافظت از داده‌های خود تقریبا اکثر کارهای لازم را انجام داده‌اید و اگر کسی از اطلاعات شما برای هرگونه کلاهبرداری سوء استفاده کند مطلع می‌شوید. اما با این وجود موضوع به همین جا ختم نمی‌شود. بازیابی اوضاع بعد از رخنه به داده‌ها ممکن است یک روند طولانی و دشوار باشد. شما باید هشیار باشید و به بررسی سوابق خود برای هرگونه فعالیت مشکوک ادامه دهید. همچنین فراموش نکنید که از خود شرکت تحت تاثیر قرار گرفته نیز کمک بگیرید.

تاریخ انتشار:

08 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/15940/%DA%86%D9%87-%D8%A8%D8%A7%DB%8C%D8%AF-%DA%A9%D8%B1%D8%AF-%D8%A7%DA%AF%D8%B1-%D8%A7%D8%B7%D9%84%D8%A7%D8%B9%D8%A7%D8%AA-%D9%85%D8%AD%D8%B1%D9%85%D8%A7%D9%86%D9%87-%D9%85%D8%A7-%D8%A7%D9%81%D8%B4%D8%A7-%D8%B4%D9%88%D8%AF