

محافظت امنیت آنلاین

چرا امنیت سایبری برای من مهم است؟

اینترنت و رسانه های اجتماعی پلتفرم های شگفت انگیزی هستند که به ما کمک میکنند معلومات را به اشتراک بگذاریم و با دوستان و فامیل در ارتباط باشیم.

با وصف این، مجرمان و سایر سازمانهای غیرقانونی نیز از آنها برای تلاش برای گرفتن پول، معلومات یا ترساندن شما استفاده میکنند. آنها میتوانند از هر کجای دنیا فعالیت کنند، به اکثر لسانها مسلط صحبت کنند و وبسایت های جعلی قانع کننده ای ایجاد کنند. آنها از طریق ایمیل، رسانه های اجتماعی و پیام با شما تماس میگیرند و سعی میکنند شما را ترسانند یا مضطرب کنند، تا شما نتوانید بصورت واضح فکر کنید. همه اینها به این معنی است که شما باید آماده باشید و همیشه از چالهای که آنها استفاده میکنند آگاه باشید.

برخی از مشکلات رایجی که ممکن است در آنلاین با آنها مواجه شوم چیست؟

اینها برخی از رایجترین وضعیتهای میباشند که ما میبینیم.

- شما یک ایمیل یا پیام مشکوک دریافت میکنید که از شما میخواهد روی یک لینک کلیک کنید.
 - این لینکها اغلب به وبسایتهای جعلی منتهی میشوند که برای سرقت معلومات ورودی یا معلومات مالی شما طراحی شده اند.
- شما یک تماس مشکوک دریافت میکنید که معلومات شخصی شما را درخواست میکند.
 - همانطور که در بالا ذکر شد، تلفون کننده وانمود میکند که از بانک شما است و معلومات شما را درخواست میکند.
- شما از کسی که وانمود میکند فردی با صلاحیت است، ارتباط برقرار میکند و سعی میکند شما را به انجام کاری وادار کند.
 - اغلب این شخص برخورد تهدید آمیز میداشته باشد.
- کسی وارد یک یا چند حساب آنلاین شما میشود (بطور مثال: ایمیل یا رسانه های اجتماعی).
 - اگر کسی وارد حساب آنلاین شما شود، آنها میتوانند معلومات را بدزدند، مسیر پرداختها را تغییر دهد و به طور بالقوه با وانمود کردن به اینکه شما هستند، دوستان یا فامیل شما را هدف قرار دهد.
- معلومات کریدیت کارت شما به سرقت رفته است، یا در یک فروش یا سرمایه گذاری جعلی فریبکاری شده است.
 - فریبکاران امیدوارند که شما یک معامله خوب را ببینید و میخواهند بدون فکر کردن پرداخت بکنید. یا شاید یک وبسایت واقعی در معرض نقض داتا قرار گرفته و معلومات شما به صورت آنلاین فاش شده باشد.

سناریوهای بیشتری در اینجا وجود دارد:

همین اکنون کمک بگیرید - مالک فضای آنلاین خود باشید

چگونه در فضای آنلاینی مصون بمانم؟

- پاسورد های طولانی و منحصر به فرد.
 - هرچه پاسورد طولانی تر باشد، قویتر است.
 - با ترکیب چهار کلمه تصادفی (مثلاً: TriangleRhinoOperationShoes) و اضافه کردن اعداد، حروف بزرگ و نمادها در صورت لزوم (مثلاً: Triangle&"Rhino"Operation2Shoes) یک پاسورد به یاد ماندنی با بیش از 16 کرکتر ایجاد کنید.
 - مهم این است که پاسورد های خود را تکرار نکنید. اگر یک مجرم یکی از پاسورد های شما را بدست آورد، آن را در حسابهای دیگر نیز امتحان خواهد کرد.
 - از یک مدیر پاسورد برای به خاطر سپردن پاسورد های خود و ایجاد پاسورد های جدید استفاده کنید.
 - پاسورد های خوب ایجاد کنید - مالک فضای آنلاین خود باشید

- **تثبیت هویت دو فکتوری داشته و انرا فعال کنید.**
 - این یک معلومات اضافی است – معمولاً یک کود روی تلفون شما – که برای ورود به یک ویسایت به آن ضرورت دارید.
 - این تکنیک فوق العاده قوی است و میتواند اکثر تلاشها برای ورود به حسابهای شما را متوقف کند.
 - ما توصیه میکنیم از یک «اب تثبیت هویت» استفاده کنید، در جاییکه از آن پشتیبانی میشود.
 - تثبیت هویت دو عاملی را تنظیم کنید (two-factor authentication (2FA) - مالک فضای آنلاین خود باشید
- **در فضای آنلاینی خصوصی بمانید.**
 - بهترین انتخاب برای مصون ماندن در رسانه های اجتماعی، فعال کردن تنظیمات حریم خصوصی شماست.
 - این کار مانع از این میشود که مردم بصورت تصادفی، از جمله مجرمان سایبری، بتوانند پستهای شما را ببینند یا برای شما پیام ارسال کنند.
 - هنوز هم مراقب نشر معلومات شخصی در باره خود، فامیل یا دوستان تان باشید.
 - مطمئن شوید که مخاطبین شما همان کسانی هستند که ادعا میکنند.
 - مراقب درخواستهای دوستی جعلی باشید. مراقب افرادی باشید که ادعا میکنند روزنامه نگار هستند یا افرادی که شما آنها را به خوبی نمیشناسید.
 - از حریم خصوصی خود در فضای آنلاینی محافظت کنید - مالک فضای آنلاین خود باشید
- **همه چیز را تازه (اپدیت) نگه دارید.**
 - وقتی تلفون، کمپیوتر یا سافت ویر خود را تازه میکنید، هرگونه خالیگاه امنیتی را نیز میپوشاند.
 - مجرمان همیشه به دنبال راههایی برای ورود هستند و این تازه کردن آسیب پذیرها را برطرف میکنند.
 - وسایل خود را مرتباً راه اندازی مجدد کنید.
 - با اپدیت های خود همسان باشید - مالک فضای آنلاین خود باشید
- **مراقب فریبکاریها باشید.**
 - بهترین توصیه این است که از این فریبکاریها آگاه باشید و مراقب آنها باشید.
 - اگر چیزی اشتباه به نظر میرسد، با شخصی که با شما تماس گرفته است، تعامل نکنید. بخصوص اگر درخواست پول کردند، حتی اگر دوستانه به نظر برسند، محتاط باشید.
 - به دنبال لینکها و آدرسهای ایمیل عجیب باشید (بطور مثال: بانک شما از یک حساب Gmail برای شما ایمیل ارسال نمیکند).
 - هرگز روی لینکهای موجود در پیامهای متنی کلیک نکنید.
 - تنها اپ ها را از فروشگاههای رسمی اپ برای وسیله خود دانلود کنید.
 - در صورت شک، مستقیماً با سازمانی که با شما تماس گرفته است تماس بگیرید و هیچ لینک یا شماره تلفونی که برای شما ارسال شده است را دنبال نکنید.
 - سعی کنید از خطرات امنیتی آنلاین برای خود، جامعه خود و هر گروهی که به آن تعلق دارید آگاه باشید.
- **از معلومات خود محافظت کنید.**
 - از اپ های پیام رسان رمزگذاری شده مانند سیگنال استفاده کنید. این کار مانع از خواندن پیامهای شما توسط هر شخص دیگر میشود.
 - معلومات را تنها در صورتی با ویسایتی به اشتراک بگذارید که آدرس آن با HTTPS شروع شود. حرف S مخفف "مصون" است و به این معنی است که هرگونه معلوماتی که بین شما و ویسایت ارسال میشود رمزگذاری شده است.
 - استفاده از یک شبکه خصوصی مجازی (VPN) را در نظر بگیرید که میتواند از داتا شما محافظت کند و مکان شما را پنهان کند.
 - اینرا معلوم کنید که اپ های شما به چه داتا و مجوزهایی دسترسی دارند. بطور مثال، یک اپ ورزشی دسترسی به تماسهای شما را ندارد.

چه کار کنم، اگر قربانی فریبکاری یا بدتر از آن قرار گرفتم؟

جاهای زیادی وجود دارد که شما میتوانید برای کمک به آنها مراجعه کنید. این سازمانها معلومات شما را با هیچ کس دیگری به اشتراک نمیگذارند، مگر اینکه شما رضایت خود را اعلام کنید.

- شما میتوانید حوادث سایبری را از طریق پورتال CERT NZ به NCSC راپور دهید و ما میتوانیم به شما کمک کنیم یا شما را با ایجنسی دیگری در ارتباط قرار دهیم:
[Report an incident | CERT NZ](#)
- اگر شما پولی از دست داده باشید، باید فوراً با بانک خود تماس بگیرید.
- پیامهای فریبکاری را میتوان به صورت مجانی به 7726، خدمتی که توسط وزارت امور داخله اداره میشود، ارسال کرد.