

ایمن ماندن در فضای مجازی

چرا امنیت سایبری برای من مهم است؟

اینترنت و رسانه‌های اجتماعی سکوه‌های شگفت‌انگیزی هستند که به ما کمک می‌کنند اطلاعات را به اشتراک گذارده و با دوستان و خانواده در ارتباط باشیم.

با این حال، مجرمان و سایر سازمان‌های غیرقانونی نیز از آنها برای بدست آوردن پول، اطلاعات یا ارباب شما استفاده می‌کنند.

آن‌ها می‌توانند از همه جای دنیا کار کنند، به اکثر زبان‌ها مسلط بوده و وبسایت‌های جعلی متقاعدکننده بسازند. آنها از طریق ایمیل، رسانه‌های اجتماعی و پیامک با شما تماس خواهند گرفت و سعی می‌کنند احساس ترس یا اضطراب در شما ایجاد کنند تا نتوانید به‌خوبی فکر کنید.

همه اینها به این معنی است که شما باید آماده بوده و همیشه از ترفندهایی که آنها استفاده می‌کنند آگاه باشید.

برخی از مشکلات رایجی که ممکن است در اینترنت با آن‌ها مواجه شوم کدامند؟

اینها برخی از رایج‌ترین موقعیت‌هایی هستند که می‌بینیم.

- یک ایمیل یا پیامک مشکوک دریافت می‌کنید که از شما می‌خواهد روی یک لینک کلیک کنید.
 - این لینک‌ها اغلب به وبسایت‌های جعلی ختم می‌شوند که برای سرقت اطلاعات ورود به سیستم یا اطلاعات مالی شما طراحی شده‌اند.
- تماس مشکوکی دریافت می‌کنید که اطلاعات شخصی شما را می‌خواهد.
 - مانند بالا، تماس‌گیرنده وانمود می‌کند که از بانک شماست و اطلاعاتی را می‌خواهد.
- شما تماسی را از شخصی دریافت می‌کنید که وانمود می‌کند یک فرد دارای مقام بالاست و سعی می‌کند شما را وادار به انجام کاری کند.
 - اغلب، این فرد به نوعی تهدید می‌کند.
- شخصی وارد یک یا چند حساب آنلاین شما می‌شود (به عنوان مثال: ایمیل یا رسانه‌های اجتماعی).
 - اگر شخصی وارد حساب آنلاین شما شود، می‌تواند اطلاعات را بدزدد، پرداخت‌ها را تغییر مسیر دهد، و احتمالاً با تظاهر به اینکه شماست، دوستان یا خانواده‌تان را هدف قرار دهد.
- جزئیات کارت اعتباری شما دزدیده می‌شود، یا در یک فروش یا سرمایه‌گذاری جعلی از شما کلاهبرداری می‌شود.
 - کلاهبرداران امیدوارند که شما معامله خوبی را ببینید و بخواهید بدون فکر پول پرداخت کنید. یا شاید یک وبسایت واقعی دچار نفوذ اطلاعاتی شده و جزئیات شما به صورت آنلاین فاش شود.

سناریوهای بیشتری در اینجا وجود دارد:

[اکنون کمک بگیرید - مالک اطلاعات آنلاین خود باشید](#)

چگونه در فضای مجازی امن بمانم؟

- رمزهای عبور طولانی و منحصر به فرد
 - هر چه رمز عبور طولانی‌تر باشد قوی‌تر است.
 - با کنار هم قرار دادن چهار کلمه تصادفی یک رمز عبور به یاد ماندنی با بیش از ۱۶ کاراکتر ایجاد کنید (به عنوان مثال: TriangleRhinoOperationShoes) و اضافه کردن اعداد، حروف بزرگ و نمادها در صورت نیاز (به عنوان مثال: Triangle&"Rhino"Operation2Shoes).
 - نکته مهم این است که رمز عبور خود را تکرار نکنید. اگر مجرمی یکی از رمزهای عبور شما را دریافت پیدا کند، آن را در حساب‌های دیگر نیز امتحان می‌کند.
 - رمزهای عبور خوب ایجاد کنید - مالک اطلاعات آنلاین خود باشید
- احراز هویت دو مرحله‌ای را فعال کنید.
 - این یک اطلاعات اضافی است - معمولاً یک کد روی تلفن‌تان - که شما باید برای وارد شدن به یک وبسایت از آن استفاده کنید.
 - این تکنیک فوق العاده قوی است و می‌تواند بسیاری از تلاش‌ها برای ورود به حساب‌های‌تان را متوقف کند.
 - توصیه می‌کنیم از «برنامه احراز هویت» در صورت پشتیبانی، استفاده کنید.
 - احراز هویت دو مرحله‌ای (FA2) را تنظیم کنید - مالک اطلاعات آنلاین خود باشید
- در فضای مجازی، خصوصی بمانید
 - بهترین گزینه برای ایمن ماندن در رسانه‌های اجتماعی این است که تنظیمات حریم خصوصی خود را فعال کنید.
 - این کار باعث می‌شود افراد تصادفی، از جمله مجرمان سایبری، نتوانند پست‌های شما را دیده یا برای شما پیام ارسال کنند.
 - از حریم خصوصی خود در فضای مجازی محافظت کنید - مالک اطلاعات آنلاین خود باشید
- همه چیز را به روز نگه دارید.
 - هنگامی که تلفن، رایانه یا نرم افزار خود را به روز می‌کنید، هر حفره امنیتی که ممکن است وجود داشته باشد را نیز پر می‌کنید.
 - مجرمان همیشه به دنبال راه‌هایی برای ورود به سیستم بوده و به روز رسانی‌ها آسیب‌پذیری‌ها را رفع می‌کنند.
 - با به روز رسانی‌های خود همراه باشید - مالک اطلاعات آنلاین خود باشید
- همیشه مراقب باشید
 - بهترین توصیه این است که از این کلاهبرداری‌ها آگاه بوده و در صورت تلاش مجرمان و تماس با شما در هر سکوی آنلاین، مراقب آنها باشید.
 - اگر هر چیزی مشکوک به نظر می‌رسد، با شخصی که با شما تماس گرفته است وارد گفتگو نشوید. به خصوص اگر آنها درخواست پول کنند، حتی اگر دوستانه به نظر می‌رسند، محتاط باشید.
 - به دنبال لینک‌ها و آدرس‌های ایمیل عجیب باشید (به عنوان مثال: بانک شما ایمیلی از حساب جی‌میل برای شما ارسال نمی‌کند).

○ در صورت شک، مستقیماً با سازمان تماس بگیرید و لینک یا شماره تلفن‌هایی که ارسال می‌کنند را دنبال نکنید.

در صورت کلاهبرداری یا شرایط بدتر از آن چه کار کنم؟

مکان‌های زیادی وجود دارد که می‌توانید برای دریافت کمک به آنها مراجعه کنید. هیچکدام از این سازمان‌ها اطلاعات شما را با فرد دیگری به اشتراک نمی‌گذارند، مگر اینکه شما رضایت خود را اعلام کنید.

- شما می‌توانید حوادث سایبری را از طریق پورتال CERT NZ به NCSC گزارش دهید و ما می‌توانیم به شما کمک کنیم یا شما را با سازمان دیگری ارجاع دهیم:
[یک حادثه را گزارش دهید | CERT NZ](#)
- اگر پول خود را از دست داده‌اید، باید بلافاصله با بانک خود تماس بگیرید.
- پیامک‌های کلاهبرداری را می‌توان به صورت رایگان به 7726، سرویسی که توسط سازمان امور داخلی کشور اداره می‌شود، ارسال کرد.