National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

ایمنی آنلاین برای سازمانتان

چرا امنیت سایبری برای گروه‌ها و سازمان‌های اجتماعی مهم است؟

این صفحه دارای توصیه‌ها و اقداماتی است که می‌توانید برای حافظت از گروه یا سازمان اجتماعی‌تان در برابر تهدیدات امنیت سایبری انجام دهید. همچنین یک راهنمای جداگانه برای ایمنی آنلاین اشخاص وجود دارد.

این توصیه بر اساس رایج ترین و جدی ترین تهدیدات است.

- به روز رسانی - نرم افزار دستگاه‌های خود را همواره به روز نگه دارید تا هر حفرهٔ امنیتی برطرف شود.
  - دستگاه‌های گروه اجتماعی یا سازمان خود را به روز نگه دارید. این مهم شامل تلفن‌ها، رایانه‌ها، روترهای WiFi و هر چیز دیگری که قابلیت اتصال به اینترنت دارد - از جمله دستگاه‌های هوشمند می‌شود.
  - در صورت امکان از به روز رسانی خودکار استفاده کنید.
- احراز هویت دو مرحله‌ای (2FA) - با نیاز به رمز عبور و یک مرحلهٔ دیگر، مانند کدِ یک برنامه در تلفن تان، امنیت بیشتری را به حساب‌های کاربری شما می‌دهد.
  - توجه: به این مورد احراز هویت چند عاملی (MFA)، تأیید دو مرحله‌ای (2SV) و بسیاری نام های دیگر نیز گفته می‌شود.
  - 2FA را در تمام حساب‌های گروه اجتماعی یا سازمانی خود فعال کنید.
  - در صورت امکان، سعی کنید از نوعی از 2FA استفاده کنید که در برابر فیشینگ مقاوم است، به این معنی که نمی‌توانید فریب خورده و اطلاعات آن را بدهید. این مهم ممکن است یک کلید امنیتی فیزیکی یا چیزی مانند اثر انگشت یا شناسهٔ چهره [فیس آی دی] باشد.
- وضعیت حساب‌های آنلاین خود را پیگیری کنید - مطمئن شوید که اعضای سابق پس از ترک گروه یا سازمان اجتماعی، دسترسی خود را به حساب‌ها حفظ نمی‌کنند.
  - اگر بیش از یک نفر به یک حساب کاربری دسترسی دارد، مطمئن شوید که همهٔ افراد نامهای کاربری مختلفی دارند و 2FA برای همهٔ آنها فعال است.
  - فهرستی از تمام حساب‌های کاربری داشته باشید و هرکدام را که لازم نیست، مثلاً زمانی که کارمندان آن سازمان را ترک می‌کنند، غیرفعال کنید.
  - تمام دستگاه‌هایی را که به اعضای خود داده‌اید ثبت کنید، و به خاطر داشته باشید که اگر آن عضو سازمان را ترک کرد دستگاه را پس گرفته و به حالت تنظیمات کارخانه درآورید. همچنین ممکن است نیاز به تغییر کدهای فیزیکی برای دسترسی به ساختمان داشته باشید.
- بررسی کنید که چه کسی به حساب‌های آنلاین شما دسترسی دارد - افراد گروه یا سازمان شما فقط باید به چیزهایی که نیاز دارند دسترسی داشته باشند.
  - اگر حساب یک نفر هک شود، این مراحل آسیبی که مهاجم می تواند وارد کند را محدود می‌کنند.
  - به طور مرتب مجوزهای غیر ضروری را بررسی و حذف کنید.
  - اگر یک حساب «ادمین» دارید که چندین نفر از آن استفاده می‌کنند، آن را رصد کنید تا فعالیت غیرمعمول نداشته باشد. سعی کنید داشتن این نوع حساب‌ها را، مخصوصاً برای کارهای روزانه، محدود کنید.
  - این قوانین برای دسترسی ادمین به دستگاه‌هایی مانند روترها نیز اعمال می‌شود.
- قراردادهای خود را با ارائه دهندگان خدمات مرور کنید - اگر کسی را استخدام کرده‌اید که خدمات فناوری اطلاعات (IT) را برای شما انجام دهد.

- اطمینان حاصل کنید که آنها از امنیت سایبری لازم برای رفع نیازهای گروه اجتماعی یا سازمان شما برخوردار هستند.

- بدانید که چگونه همه حساب‌ها و سیستم‌های شما با هم کار می‌کنند – درک اتصالات به شما کمک می‌کند بدانید مهاجم از کجا می‌تواند وارد شود.
  - اتصالات بین سیستم‌های خود را مرور کنید، به عنوان مثال، ایمیل، فضای ذخیره سازی ابری، و پلتفرم‌های حسابداری.
  - برای امنیت آنلاین بیشتر، از یک شبکهٔ خصوصی مجازی (VPN) استفاده کنید. استفاده از VPN فعالیت آنلاین شما را از هر کسی که ممکن است سعی کند شما را ردیابی کند پنهان می‌کند. این امر به ویژه زمانی سودمند است که اعضای گروه یا سازمان اجتماعی شما از راه دور متصل شوند.

- اعضای خود را «مطلع سایبری» نگاه دارید - احتمال اینکه افراد گروه یا سازمان اجتماعی شما مورد هدف قرار گیرند بیشتر از سیستم‌های شماست.
  - کلیهٔ کارکنان را در زمینهٔ امنیت سایبری اولیه آموزش دهید. وب‌سایت مالک اطلاعات آنلاین خود باشید مالک اطلاعات آنلاین خود باشید | NCSC طیف گسترده ای از توصیه‌ها و نکات برای کمک به حفظ امنیت شما در فضای آنلاین و نحوهٔ تشخیص کلاهبرداری دارد.
  - به آنها یادآوری کنید که این مهم برای حساب‌های شخصی آنها و همچنین حساب‌هایی که برای سازمان شما استفاده می‌کنند مهم است.
  - ما یک دستورالعمل برای افراد داریم تا از امنیت آنلاین خود نیز محافظت کنند.

- برای یک حادثه برنامه ریزی کنید - داشتن یک برنامهٔ واکنش برای جلوگیری از وحشت مردم هنگام وقوع یک حادثه، مهم است.
  - یک طرح واکنش به حادثه مشخص می‌کند که هر کسی در طول یک حادثه چه کاری انجام می‌دهد. الگوها در اینجا موجود هستند مدیریت حوادث | NCSC
  - برنامه‌ای را برای اقدامات در صورت خرابی تلفن‌ها، رایانه‌ها یا سایر سیستم‌ها در نظر بگیرید. این برنامه را به روز نگه دارید.
  - اطلاعات تماس همهٔ افراد مورد نیاز و جزئیات پشتیبان را در صورت خرابی راه اصلی تماس با آنها (مانند ایمیل) نگه دارید.
  - در صورتی که امکان دسترسی به برنامه نباشد، آن را در جایی خارج از سیستم خود نیز نگه دارید.