National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

حفظ امنیت فضای آنلاینی سازمان شما

چرا امنیت سایبری برای گروهها و سازمانهای اجتماعی مهم است؟

این صفحه شامل توصیه ها و برخی از اقداماتی است که شما میتوانید برای محافظت از گروه یا سازمان اجتماعی خود در برابر تهدیدات امنیت سایبری انجام دهید. همچنان یک راهنمای جداگانه برای اشخاص وجود دارد.

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

- تازه کردن (اپدیت) – سافت ویر را در وسیله های خود تازه نگه دارید تا هرگونه خالیگاه امنیتی را برطرف کنید.
  - وسیله های گروه یا سازمان اجتماعی خود را تازه نگه دارید. این شامل تلیفون ها، کمپیوتر ها، روترهای WiFi و هر چیز دیگری که به اینترنت متصل میشود – از جمله وسیله های هوشمند – میشود.
  - در صورت امکان از تازه کردن های اتومات استفاده کنید.
- تثبیت هویت دو عاملی ((Two-factor authentication (2FA) – با نیاز به پاسورد و یک مرحله دیگر، مانند کود از یک اپ در تلیفون شما، امنیت بیشتری را به حسابهای شما اضافه میکند.
  - توجه: این روش با نامهای تثبیت هویت چند عاملی ((multi-factor authentication (MFA)، تأیید هویت دو مرحله ای ((two-step verification (2SV) و بسیار نامهای دیگر شناخته میشود.
  - 2FA را روی تمام حساب های گروه یا سازمان خود فعال کنید.
  - در صورت امکان، کوشش کنید از نوعی از 2FA استفاده کنید که در برابر فیشینگ مقاوم باشد، به این معنی که شما فریب نخورید و آن را تسلیم ندهید. این میتواند یک کلید امنیتی فیزیکی یا چیزی شبیه اثر انگشت یا شناسای چهره باشد.
- حسابهای آنلاینی خود را تعقیب کنید – مطمئن شوید که اعضای سابق پس از ترک کردن وظیفه در گروه یا سازمان، دسترسی خود را به حساب ها حفظ نمیکنند.
  - اگر بیشتر از یک نفر را دارید که به یک حساب کاربری دسترسی دارند، مطمئن شوید که همه آنها دارای نامهای کاربری متفاوت هستند و همه 2FA را روشن کرده اند.
  - لستی از تمام حسابهای کاربری داشته باشید و هر کدام را که لازم نیست، مانند وقتیکه کارمندان کار را ترک میگویند، انرا غیرفعال کنید.
  - از هر وسیله که به اعضای کاری خود داده اید، فهرستی تهیه کنید و به یاد داشته باشید که اگر آن شخص سازمان را ترک کرد، آنها را پس بگیرید و به تنظیمات سابقه کارخانه برگردانید. شما همچنان ممکن است لازم باشد کودهای فیزیکی برای دسترسی به عمارت را تغییر دهید.
- بررسی کنید چه کسی به حسابهای آنلاینی شما دسترسی دارد – افراد گروه یا سازمان شما فقط باید به چیز هایی که ضرورت دارند دسترسی داشته باشند.
  - اگر حساب یک نفر «هک» شود، این مراحل آسیبی را که یک مهاجم میتواند وارد کند، محدود میکند.
  - به طور منظم مجوز های غیرضروری را بررسی و حذف کنید.
  - اگر شما یک حساب «مدیر» دارید که چندین نفر از آن استفاده میکنند، آن را برای فعالیتهای غیرمعمول زیر نظر داشته باشید. سعی کنید داشتن این نوع حسابها را، بخصوص برای کار های روزانه، محدود کنید.
  - این قوانین در باره دسترسی مدیر به دستگاههایی مانند روترها نیز اعمال میشود.

- قرارداد های خود را با فراهم کنندگان خدمات بررسی کنید – اگر کسی را برای اجرای خدمات تکنالوژی خود استخدام کرده اید.
    - مطمئن شوید که آنها دارای حفاظتهای امنیتی سایبری برای برآورده کردن ضرورت های گروه یا سازمان اجتماعی شما هستند.
- بدانید که چگونه همه حسابها و سیستمهای شما با هم کار میکنند – درک ارتباطات به شما کمک میکند تا بدانید که یک مهاجم از کجا میتواند وارد شود.
    - ارتباطات بین سیستمهای خود، به عنوان مثال، ایمیل، ذخیره فضای ابری و پلتفورمهای حسابداری را بررسی کنید.
    - برای امنیت بیشتر آنلاینی، استفاده از یک شبکه خصوصی مجازی ((Virtual Private Network (VPN) را در نظر بگیرید. استفاده از VPN فعالیت آنلاین شما را از هر کسی که ممکن است سعی در ردیابی شما داشته باشد، پنهان میکند. این امر بخصوص در صورتی که هر یک از اعضای گروه یا سازمان اجتماعی شما از راه دور متصل شوند، مفید است.
- افراد خود را "هوشیار سایبری" نگه دارید – افراد گروه یا سازمان اجتماعی شما بیشتر از سیستمهای شما در معرض هدف قرار میگیرند.
    - تمام کارمندان را در زمینه امنیت سایبری آموزش ساده بدهید. مالک ویبسایت آنلاین خود باشید Own Your Online | NCSC طیف گستردهای از توصیه ها و نکات را برای کمک به حفظ امنیت آنلاینی خود و طریقه تشخیص فریبکاریها را فراهم میکند.
    - به آنها یادآوری کنید که این موضوع هم برای حسابهای شخصی شان و هم برای حسابهای کاربری سازمان شما مهم است.
    - ما برای افراد نیز راهنمایی داریم: Keeping safe online | Ministry for Ethnic Communities
- داشتن یک پلان برای یک حادثه – داشتن یک پلان واکنش به حادثه برای جلوگیری از وحشت افراد هنگام وقوع حادثه مهم است.
    - یک پلان واکنش به حادثه مشخص میکند که چه کسی در طول یک حادثه چه کاری انجام میدهد. قالبها در اینجا موجود است مدیریت حادثه | NCSC.
    - یک پلان برای اقدامات لازم در صورت خرابی تلیفونها، کمپیوتر ها یا سایر سیستمها را در نظر بگیرید. این پلان را تازه نگه دارید.
    - معلومات تماس همه افراد مورد ضرورت و معلومات پشتیبان را در صورت خرابی راه اصلی تماس با آنها (مانند ایمیل) نگه دارید.
    - پلان را در یک جایی خارج از سیستم خود نیز نگه دارید، وقتیکه نمیتوانید به آن دسترسی داشته باشید.