Community Resilience
to Foreign Interference

National Cyber Security Centre

اپنے ادارے کو آن لائن محفوظ رکھنا

کمیونٹی گروپوں اور تنظیموں کے لئے سائبر سیکورٹی کیوں اہم ہے؟

اس صفحے میں مشورہ اور کچھ ایسے اقدامات ہیں جو آپ اپنے کمیونٹی گروپ یا تنظیم کو سائبر سیکیورٹی کے خطرات سے بچانے کے لئے اٹھا سکتے ہیں۔ افراد کے لیے آن لائن خود کو محفوظ رکھنے کے لئے ایک علیحدہ گائیڈ بھی موجود ہے۔

یہ مشورہ عام ترین اور سنگین ترین خطرات کے حوالے سے ہے۔

اپ ڈیٹس

سیکیورٹی میں کسی بھی کمی کو دور کرنے کے لئے اپنے آلات پر سافٹ ویئر کو تازہ ترین رکھیں۔

- اپنے کمیونٹی گروپ یا تنظیم کے آلات کو اپ ڈیٹ رکھیں۔ اس میں فون، کمپیوٹر، وائی فائی روٹر اور انٹرنیٹ سے منسلک کوئی بھی چیز شامل ہے - بشمول اسمارٹ ڈیوائسز۔
- جہاں ممکن ہو خودکار اپ ڈیٹس استعمال کریں۔

ٹو فیکٹر اتھینٹیکیشن یا تصدیق (2FA)

پاس ورڈ کے علاوہ ایک اوراضافی قدم کے ذریعے آپ کے اکاؤنٹس میں اضافی سیکورٹی فراہم کرتا ہے، جیسے کہ آپ کے فون پر کسی ایپ سے ایک کوڈ وصول ہونا۔

- نوٹ: اسے ملٹی فیکٹر اتھینٹیکیشن یا تصدیق (MFA)، دو مراحل کی تصدیق (two-step verification - 2SV) اور بہت سے دیگر ناموں سے بھی جانا جاتا ہے۔
- اپنے کمیونٹی گروپ یا تنظیم کے تمام اکاؤنٹس پر 2FA کو آن کریں۔
- اگر ممکن ہو تو ، 2 FA کی ایک ایسی شکل استعمال کرنے کی کوشش کریں جو جعل سازی کے خلاف مزاحمت کرتی ہو، جس کا مطلب ہے کہ آپ کے لاگ ان تک رسائی آپ سے دھوکے سے حاصل نہیں کی جا سکتی۔ یہ فزیکل سکیورٹی keyہو سکتی ہے یا فنگر پرنٹ یا فیس آئی ڈی کی طرح کی چیز ہو سکتی ہے۔

اپنے آن لائن اکاؤنٹس پر نظر رکھیں

اس بات کو یقینی بنائیں کہ سابق ارکان کے کمیونٹی گروپ یا تنظیم چھوڑنے کے بعد انہیں کمینٹی گروپ یا تنظیم کے اکاؤنٹس تک رسائی نہ ہو۔

- اگر آپ کے پاس ایک ہی اکاؤنٹ تک رسائی حاصل کرنے والے ایک سے زیادہ افراد ہیں تو، اس بات کو یقینی بنائیں کہ ان سب کے پاس مختلف لاگ ان ہیں، اور سبھی کے پاس 2FA آن ہے۔
- صارفین کے تمام اکاؤنٹس کی ایک فہرست بنائیں اور کسی بھی ایسے اکاؤنٹ کو غیر فعال کریں جس کی ضرورت نہیں ہے، جیسے جب عملہ چھوڑ جائے۔
- اپنے ممبروں کو دیئے گئے تمام آلات کا ایک رجسٹر رکھیں اور اگر کوئی شخص تنظیم چھوڑ دیتا ہے تو ان آلات کو واپس حاصل کرنا اور فیکٹری ری سیٹ کرنا یاد رکھیں۔ آپ کو عمارت میں رسائی کے فزیکل کوڈ تبدیل کرنے کی بھی ضرورت ہوسکتی ہے۔

چیک کریں کہ آپ کے آن لائن اکاؤنٹس تک کس کی رسائی ہے

آپ کے کمیونٹی گروپ یا تنظیم کے لوگوں کو صرف ان چیزوں تک رسائی حاصل ہونی چاہئے جن کی انہیں ضرورت ہے۔

- اگر کسی ایک شخص کا اکاؤنٹ ہیک ہو جاتا ہے تو یہ اقدامات حملہ آور کے نقصان پہنچانے کی صلاحیت کو محدود کرتے ہیں۔
- غیر ضروری اجازتوں کو باقاعدگی سے چیک کریں اور ہٹا دیں۔
- اگر آپ کے پاس ایک ہی "ایڈمن" اکاؤنٹ ہے جو متعدد افراد استعمال کرتے ہیں تو، غیر معمولی سرگرمی کے لئے اس کی نگرانی کریں۔ خاص طور پر روزمرہ کے کاموں کے لئے اس قسم کے اکاؤنٹس کی تعداد کو کم سے کم رکھنے کی کوشش کریں۔
- یہ قواعد آلات تک رسائی کے لیے ایڈمن اکاؤنٹس پر بھی لاگو ہوتے ہیں، جیسے routers۔

اگر آپ نے اپنے لئے آئی ٹی خدمات چلانے کے لئے کسی کی خدمات حاصل کی

ہیں تو سروس فراہم کنندگان کے ساتھ اپنے معاہدوں کا جائزہ لیں۔

- اس بات کو یقینی بنائیں کہ آپ کے کمیونٹی گروپ یا تنظیم کی ضروریات کو پورا کرنے کے لئے ان کے پاس سائبر سیکیورٹی تحفظ موجود ہے۔

یہ جانیں کہ آپ کے تمام اکاؤنٹس اور سسٹم ایک ساتھ کیسے کام کرتے ہیں

ان کنکشنز کو سمجھنے سے آپ کو یہ جاننے میں مدد ملتی ہے کہ حملہ آور کہاں سے داخل ہوسکتا ہے۔

- اپنے سسٹم کے مابین کنیکشنز کا جائزہ لیں، مثال کے طور پر، ای میل، کلاؤڈ اسٹوریج، اور اکاؤنٹنگ پلیٹ فارم۔
- اضافی آن لائن حفاظت کے لئے ورچوئل پرائیویٹ نیٹ ورک (وی پی این) استعمال کرنے پر غور کریں۔ وی پی این کا استعمال آپ کی آن لائن سرگرمی کو کسی بھی ایسے شخص سے چھپاتا ہے جو آپ کو ٹریک کرنے کی کوشش کرسکتا ہے۔ یہ خاص طور پر اس صورت میں زیادہ بہتر ہے اگر آپ کے کمیونٹی گروپ یا تنظیم کا کوئی بھی رکن ریموٹ کنیکٹ ہوتا ہے۔

اپنے لوگوں کو 'سائبر اسمارٹ' بنائیں

آپ کے کمیونٹی گروپ یا تنظیم کے لوگوں کو آپ کے سسٹمز کے مقابلے میں نشانہ بنائے جانے کا زیادہ امکان ہے۔

- تمام عملے کو بنیادی سائبر سیکورٹی کی تربیت دیں۔ Own Your Online ویب سائٹ Own Your Online | NCSC پر اپنے آپ کو آن لائن محفوظ رکھنے اور فریب کی نشاندہی کرنے میں مدد کے لئے مشورے اور تجاویز کی ایک وسیع فہرست ہے۔
- انہیں یاد دلائیں کہ یہ ان کے ذاتی اکاؤنٹس کے ساتھ ساتھ ان اکاؤنٹس کے لئے بھی اہم ہے جو وہ آپ کی تنظیم کے لئے استعمال کرتے ہیں۔
- ہمارے پاس انفرادی لوگوں کے لئے بھی ایک گائیڈ موجود ہے تاکہ وہ خود کو آن لائن محفوظ رکھ سکیں۔

حادثے کی منصوبہ بندی

جب کوئی حادثہ پیش آتا ہے تو لوگوں کو گھبرانے سے بچانے کے لئے ایک جوابی منصوبہ رکھنا ضروری ہے۔

- ایک انسیڈنٹ رسپانس پلان/جوابی منصوبہ اس بات کی نشاندہی کرتا ہے کہ کسی حادثے کے دوران کون شخص کیا کام کرتا ہے۔ ٹیمپلیٹس یہاں دستیاب ہیں NCSC | انسیڈنٹ مینجمنٹ
- اگر فون، کمپیوٹر، یا دیگر سسٹم ناکام ہوجاتے ہیں تو کیا کرنا ہے، اس کے لئے ایک منصوبہ شامل کریں۔ اس منصوبے کو اپ ڈیٹ رکھیں۔
- تمام مطلوبہ افراد کی رابطے کی تفصیلات اکٹھا کریں اور ایک بیک اپ طریقہ تیارکریں تاکہ وہ اس صورت میں کام آ سکے جب ان افراد سے رابطہ کرنے کا اہم طریقہ ٹوٹ جائے(جیسے ای میل)۔
- منصوبے کو اپنے سسٹم سے باہر بھی کسی جگہ محفوظ رکھیں ، تاکہ وہ اس صورت میں کام آ سکے جب سسٹم آپ کی پہنچ سے باہر ہو۔