National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

آن لائن محفوظ رہنا

سائبر سکیورٹی میرے لئے کیوں اہم ہے؟

انٹرنیٹ اور سوشل میڈیا حیرت انگیز پلیٹ فارم ہیں، جو معلومات کے اشتراک، اور دوستوں اور خاندان کے افراد سے رابطے میں رہنے میں ہماری مدد کرتے ہیں۔

تاہم، جرائم پیشہ افراد اور دیگر غیر قانونی ادارے ان کو آپ کی رقم، معلومات حاصل کرنے یا آپ کو دھمکانے کے لئے بھی استعمال کرنے کی کوشش کرتے ہیں۔

وہ دنیا میں کہیں سے بھی کام کر سکتے ہیں، وہ زیادہ تر زبانیں روانی سے بول سکتے ہیں اور قائل کرنے والی جعلی ویب سائٹس بناتے ہیں۔ وہ آپ سے ای میل، سوشل میڈیا اور ٹیکسٹ میسج کے زریعہ رابطہ کریں گے،اور وہ آپ کو خوفزدہ کرنے یا پریشانی کا احساس دلانے کی کوشش کریں گے تاکہ آپ واضح طور پر سوچ نہ سکیں۔

اس سب کا مطلب یہ ہے کے آپ تیار رہیں اور ہمیشہ ان کی چالوں سے ،جو وہ استعمال کرتے ہیں، اگاہ رہیں۔

وہ کون سے کچھ عام مسائل ہیں جن سے میرا آن لائن سامنا ہو سکتا ہے؟

یہ کچھ عام حالات ہیں جو ہم زیادہ تر دیکھتے ہیں۔

- آپ کو ایک مشکوک ای میل یا ٹیکسٹ میسج ملتا ہے اور کسی لنک پر کلک کرنے کو کہا جاتا ہے۔
    - یہ لنکس اکثر جعلی ویب سائٹس کی طرف لے جاتے ہیں جو آپ کے لاگ ان یا مالی تفصیلات کو چرانے کے لیے بنائی گئی ہیں۔
- آپ کو ایک مشکوک کال موصول ہوتی ہے جس میں ذاتی معلومات طلب کی جاتی ہیں۔
    - جیسا کہ اوپربتایا گیا ہے، فون کرنے والا آپ کے بینک سے ہونے کا بہانہ کرے گا اور معلومات طلب کرے گا۔
- آپ سے کوئی ایسا شخص رابطہ کرتا ہے جو ایک بااختیار شخص ہونے کا بہانہ کر رہا ہے اور آپ سے کچھ کروانے کی کوشش کر رہا ہے۔
    - اکثر وہ شخص کسی نہ کسی قسم کی دھمکی دیتا ہے۔
- کوئی آپ کے ایک یا زیادہ آن لائن اکاؤنٹس میں داخل ہو جاتا ہے (مثال کے طور پر: ای میل یا سوشل میڈیا)۔
    - اگر کوئی آپ کے آن لائن اکاؤنٹ میں داخل ہوجاتا ہے تو وہ معلومات چوری کر سکتا ہے، ادائیگیوں کو ری ڈائریکٹ کر سکتا ہے، اور ممکنہ طور پر آپ کا بہانہ کرکے آپ کے دوستوں یا خاندان کو نشانہ بنا سکتا ہے۔
- آپ کے کریڈٹ کارڈ کی تفصیلات چوری ہو گئی ہیں، یا آپ کو جعلی فروخت یا سرمایہ کاری کے ذریعے رقم کا دھوکہ دیا گیا ہے۔
    - سکیمرز یا دھوکہ دینے والے افراد یہ امید کر رہے ہیں کہ آپ ایک اچھا سودا دیکھ کر بغیر سوچے سمجھے ادائیگی کرنا چاہیں گے۔ یا یہ ہو سکتا ہے کہ ممکنہ طور پر ایک حقیقی ویب سائٹ پر ڈیٹا کی خلاف ورزی ہوئی ہے اور آپ کی تفصیلات آن لائن لیک ہو گئی ہیں۔

یہاں مزید منظرنامے ہیں:
ابھی مدد حاصل کریں - اپنے آن لائن اکاؤنٹس کی حفاظت کریں

میں آن لائن کیسے محفوظ رہوں؟

- **طویل اور منفرد پاس ورڈز۔**
  - پاس ورڈ جتنا لمبا ہوگا اتنا ہی مضبوط ہوگا۔
  - چار بے ترتیب الفاظ کو ایک ساتھ جوڑ کر (مثال کے طور پر: TriangleRhinoOperationShoes) اور اگر ضرورت ہو تو اعداد، بڑے حروف اور علامتیں شامل کر کے 16 سے زیادہ حروف کا یاد رکھنے والا پاس ورڈ بنائیں (مثال کے طور پر: Triangle&"Rhino"Operation2Shoes)۔
  - اہم بات یہ ہے کہ اپنے پاس ورڈ نہ دہرائیں۔ اگر کسی مجرم کو آپ کا پاس ورڈ مل جاتا ہے تو وہ اسے دوسرے اکاؤنٹس پر بھی آزمائیں گے۔
  - اپنے پاس ورڈ یاد رکھنے اور نئے پاس ورڈ بنانے کے لیے پاس ورڈ مینجر استعمال کریں۔
  - اچھے پاس ورڈ بنائیں - اپنے آن لائن اکاؤنٹس کی حفاظت کریں
- **ٹو فیکٹر اتھینٹیکیشن (two-factor authentication) کو آن کریں۔**
  - یہ معلومات کا ایک ایسا اضافی ٹکڑا ہے – عام طور پر آپ کے فون پر ایک کوڈ کی شکل میں – جو آپ کو ویب سائٹ میں لاگ ان ہونے کے لیے درکار ہے۔
  - یہ تکنیک ناقابل یقین حد تک مضبوط ہے اور آپ کے اکاؤنٹس میں داخل ہونے کی زیادہ تر کوششوں کو روک سکتی ہے۔
  - ہم ایک 'Authenticator ایپ' استعمال کرنے کی تجویز کرتے ہیں، جو اس چیز کو سپورٹ کرتی ہے۔
  - two-factor authentication (2FA) سیٹ اپ کریں - اپنے آن لائن اکاؤنٹس کی حفاظت کریں
- **آن لائن جا کر خود کو پرائیویٹ رکھیں۔**
  - سوشل میڈیا پر محفوظ رہنے کا بہترین طریقہ یہ ہے کہ آپ اپنی پرائیویسی سیٹنگز کو آن کریں۔
  - یہ سیٹنگز انجانے لوگوں کو، بشمول سائبر کریمینلز، آپ کی پوسٹس دیکھنے یا آپ کو پیغامات بھیجنے سے روکیں گی۔
  - اب بھی اپنے، اپنے گھرانے اور دوستوں کے بارے میں ذاتی معلومات پوسٹ کرنے میں احتیاط برتیں۔
  - اس بات کو یقینی بنائیں کہ رابطہ کرنے والے شخص وہی ہیں جو وہ ہونے کا دعوی کرتے ہیں۔
  - جعلی فرینڈ ریکوئیسٹس پر نظر رکھیں۔ ان لوگوں سے محتاط رہیں جو صحافی ہونے کا دعویٰ کرتے ہیں یا ایسے دیگر لوگ جنہیں آپ اچھی طرح سے نہیں جانتے۔
  - آن لائن اپنی پرائیویسی کی حفاظت کریں - اپنے آن لائن اکاؤنٹس کی حفاظت کریں
- **ہر چیز کو اپ ڈیٹ رکھیں۔**
  - جب آپ اپنے فون، کمپیوٹر یا سافٹ وئیر کو اپ ڈیٹ کرتے ہیں تو یہ ممکنہ سیکیورٹی کوتاہیوں کو بھی ختم کرتا ہے۔
  - مجرم ہمیشہ آپ کے اکاؤنٹس میں داخل ہونے کے طریقے تلاش کرتے رہتے ہیں اور اپ ڈیٹس ایسی کمزوریوں کو دور کرتی ہیں۔
  - اپنے آلات کو باقاعدگی سے ری سٹارٹ کریں۔
  - اپنی اپ ڈیٹس کو تروتازہ رکھیں - اپنے آن لائن اکاؤنٹس کی حفاظت کریں

- **اسکیمز (scams) سے با خبر رہیں۔**
  - بہترین مشورہ یہ ہے کہ ان اسکیمز (scams) سے آگاہ رہیں اور اگر مجرم کسی بھی آن لائن پلیٹ فارم پر آپ سے رابطہ کرنے کی کوشش کریں تو ان پر نظر رکھیں۔
  - اگر کچھ غلط لگتا ہے تو، اس شخص کے ساتھ مشغول نہ ہوں جس نے آپ سے رابطہ کیا ہے۔ خاص طور پر اس وقت محتاط رہیں جب وہ پیسے مانگیں، چاہے وہ دوستانہ لگیں۔
  - عجیب لنکس اور ای میل پتوں سے چوکنا رہیں (مثال کے طور پر: آپ کا بینک آپ کو جی میل اکاؤنٹ سے ای میل نہیں بھیجے گا)۔
  - ٹیکسٹ میسجز میں موجود لنکس پر کبھی کلک نہ کریں
  - اپنے ڈیوائس پر ہمیشہ آفیشل ایپ اسٹورز ہی سے ایپس ڈاؤن لوڈ کریں۔
  - اگر شک ہو تو ادارے سے براہ راست رابطہ کریں اور بھیجے گئے کسی بھی لنک یا فون نمبر کی پیروی نہ کریں۔
  - اپنے لئے، اپنی کمیونٹی اور خود سے جڑے کسی بھی گروپ کے لئے درپیش آن لائن سیکیورٹی خطرات سے آگاہ رہنے کی کوشش کریں۔
- **اپنی معلومات کی حفاظت کریں۔**
  - انکرپٹڈ میسجنگ ایپس استعمال کریں، جیسے Signal۔ ایسا کرنے سے لوگ آپ کے پیغامات پڑھ نہیں سکیں گے۔
  - صرف اس ویب سائٹ کے ساتھ معلومات کا اشتراک کریں جس کا ایڈریس HTTPS سے شروع ہوتا ہو۔ S سے مراد "محفوظ" ہے اور اس کا مطلب ہے کہ آپ اور ویب سائٹ کے درمیان بھیجی گئی کوئی بھی معلومات خفیہ یا encrypted رہیں گی۔
  - ایک ورچوئل پرائیویٹ نیٹ ورک (وی پی این) استعمال کرنے پر غور کریں جو آپ کے ڈیٹا کی حفاظت کرسکتا ہے اور آپ کے مقام کو چھپا سکتا ہے۔
  - چیک کریں کہ آپ کی ایپس کو کون سے ڈیٹا اور اجازتوں تک رسائی حاصل ہے۔ مثال کے طور پر ، فٹنس ایپ کو آپ کے رابطوں تک رسائی کی ضرورت نہیں ہے۔

اگر میں دھوکہ دہی کا شکار یا اس سے بدتر صورتحال سے دوچار ہو جاتا ہوں تو میں کیا کروں؟

بہت ساری جگہیں ہیں جہاں آپ مدد کے لیے جا سکتے ہیں۔ یہ تمام ادارے آپ کی تفصیلات کسی اور کے ساتھ شیئر نہیں کریں گے، جب تک کہ آپ اپنی رضامندی نہ دیں۔

- آپ CERT NZ پورٹل کے ذریعے NCSC کو سائبر واقعات کی اطلاع دے سکتے ہیں اور ہم آپ کی مدد کر سکتے ہیں یا کسی دوسری ایجنسی سے آپ کا رابطہ کروا سکتے ہیں:
  واقعے کی اطلاع دیں | CERT NZ
- اگر آپ کے پیسے ضائع ہو گئے ہیں، تو آپ کو فوری طور پر اپنے بینک سے رابطہ کرنا چاہیے۔
- سکیم (scam) ٹیکسٹ میسجز کو بلا معاوضہ 7726 پر فارورڈ کیا جا سکتا ہے، یہ سروس ڈیپارٹمنٹ آف انٹرنل افیئرز کی جانب سے چلائی جاتی ہے۔