[FRONTCOVER]

[Start Community Language Document 1]

سائبر سے واقفیت

[یعنی انٹرنیٹ پر پیغام رسانی سے آگاہی]

نیشنل سائبر سیکیورٹی سینٹر کی جانب سے متبادل اشاعت کی ترتیب بندی۔

اس مواد کو لیہڈ اسکاٹ لینڈ نے اسکاٹش گورنمنٹ کے سائبر ریزیلئنس یونٹ کی مالی معاونت کے ذریعے پارٹنرز کے ساتھ مل کر تیار کیا ہے۔

یہ ہدایت نامہ نیشنل سائبر سیکیورٹی سینٹر کی ویب سائیٹ پر دستیاب مواد پر مبنی ہے۔

ان معلومات کو 7 کمیونٹی زبانوں کی تحریر میں تقسیم کیا گیا ہے جو یہ ہیں:

- یہ تحریر جس میں ایک تعارف اور ان 6 اقدامات کا جائزہ شامل ہے جو آپ اپنی آن لائن سیکیورٹی کو بہتر بنانے کے لیے اٹھا سکتے ہیں۔
- اس کے بعد 6 اقدامات اٹھانے کے بارے میں مفصل انفرادی تحریریں موجود ہیں۔
- تمام مذکورہ لنکس تک رسائی نیشنل سائبر سیکیورٹی سینٹر کی یہ ویب سائٹ وزٹ کر کے حاصل کی جا سکتی ہے۔

https://www.ncsc.gov.uk/cyberaware/

اپنی آن لائن سیکیورٹی کو بہتر بنانے کے 6 طریقے

کورونا وائرس کی وجہ سے اس سال لوگ اپنا زیادہ تر وقت آن لائن گزار رہے ہیں۔

اس کا مطلب یہ ہے کہ ہیکرز [کسی دوسرے شخص کے کمپیوٹر تک بلا اجازت رسائی حاصل کرنے والے] کے لئے سائبر حملوں کا زیادہ موقع موجود ہوتا ہے۔ وہ یہ کام اکثر اوقات ذیل کا استعمال کرتے ہوئے لوگوں اور کاروباری اداروں کو نشانہ بنا کر انجام دیتے ہیں۔

- ای میل اور ویب سائیٹ کے ذریعے دھوکہ دہی۔
- میل ویئر۔ یہ ایک سافٹ ویئر ہے جو آپ کے ڈیوائس کو نقصان پہنچا سکتا ہے یا کسی ہیکر کو اندر داخل ہونے دیتا ہے۔

اگر ہیکرز آپ کے ڈیوائس یا اکاؤنٹس میں داخل ہو جائیں تو وہ آپ کے پیسوں، آپ کی ذاتی معلومات یا آپ کے کاروبار سے متعلق معلومات تک رسائی حاصل کر سکتے ہیں۔

آپ چھ اقدامات اٹھا کر اپنی سائبر سیکیورٹی کو بہتر بنا سکتے / سکتی ہیں۔

اقدام 1- اپنی ای میل کے لئے ایک مضبوط اور متفرق پاس ورڈ استعمال کریں۔

اقدام 2 - 3 بے ترتیب الفاظ استعمال کر کے مضبوط پاس ورڈ بنائیں۔

اقدام 3 - اپنے پاس ورڈز کو اپنے براؤزر میں محفوظ کر لیں۔

اقدام 4 - دو عنصر کی توثیق (2 ایف اے) کو آن کر دیں۔

اقدام 5 - اپنی ڈیوائس اپ ڈیٹ کریں۔

اقدام 6 - اپنے ڈیٹا کا بیک اپ تیار کریں۔

[End Community Language Document 1]

[Start Community Language Document 2]

اقدام 1 - اپنی ای میل کے لئے ایک مضبوط اور متفرق پاس ورڈ استعمال کریں

اگر کوئی ہیکر آپ کے ای میل میں داخل ہو جائے تو وہ آپ کے دیگر اکاؤنٹس کے پاس ورڈز اور رسائی کی معلومات، جو آپ نے اپنے اور اپنے کاروبار کے بارے میں محفوظ کی ہوئی ہوتی ہیں کو دوبارہ سے مرتب کر سکتا ہے۔

آپ کی ای میل کا پاس ورڈ مضبوط اور آپ کے دیگر تمام پاس ورڈز سے مختلف ہونا چاہئے۔ اس سے نقب لگانا یا اندازہ لگانا مشکل ہو جائے گا۔

ایک مضبوط اور منفرد پاس ورڈ بنانے کے لئے تین بے ترتیب الفاظ کا استعمال کرنا ایک اچھا طریقہ ہے جو آپ کو یاد ہو گا۔ اگلی تحریر میں ہم اس کا مزید تفصیل سے جائزہ لیں گے۔

آپ کو اپنے دیگر اہم اکاؤنٹس مثلاً "بینکنگ یا سوشل میڈیا کی بھی حفاظت کرنی چاہئے۔

ای میل اتنی اہم کیوں ہوتی ہے؟

ای میل آپ کے سب سے اہم اکاؤنٹس میں سے ایک ہے۔ لیکن ہیکرز آپ کی ای میلز پر نظر کیوں رکھتے ہیں؟

سوچئے کہ اگر کوئی ہیکر آپ کی ای میل میں داخل ہو جاتا ہے۔

اب وہ ان معلومات تک رسائی حاصل کر سکتا ہے جو آپ نے اپنے بارے میں محفوظ کی ہوئی ہیں یا وہ آپ کے جعلی روپ میں لوگوں سے رابطہ کر سکتا ہے۔

لیکن سب سے بدترین بات یہ ہے کہ وہ کسی بھی آن لائن اکاؤنٹ تک آپکی رسائی کو لاک کر سکتے ہیں۔

وہ آپ کے کسی بھی اکاؤنٹ میں جا کر 'بھولے ہوئے پاس ورڈ' کی خصوصیت کا استعمال کر کے ایسا کر سکتے ہیں۔

آپ کے پاس ورڈز کو دوبارہ سے ترتیب دینے کے لیے یہ آپ کو لنک کے ساتھ ایک ای میل بھیجتا ہے ہیکر جس کو آپ کا اکاؤنٹ لاک کرنے کے لئے استعمال کر سکتا ہے۔

ایک بار جب وہ ایک پاس ورڈ دوبارہ سے ترتیب دے لیتا ہے تو وہ آپ کے دیگر اکاؤنٹس کے پاس ورڈز بھی دوبارہ سے ترتیب دینا جاری رکھ سکتا ہے۔

لہذا آپ اپنی ای میل کی حفاظت کرنے اور ہیکرز کو اپنے تمام آن لائن اکاؤنٹس سے دور رکھنے سے کس طرح مستفید ہو سکتے ہیں؟

اپنی ای میل کے لئے ایک مضبوط پاس ورڈ استعمال کریں اور اس بات کو یقینی بنائیں کہ آپ کی ای میل کا پاس ورڈ آپ کے دیگر تمام پاس ورڈز جو آپ استعمال کرتے ہوں سے مختلف ہو۔

اس کا مطلب یہ ہے کہ اگر کوئی آپ کے کسی اور اکاؤنٹ کا پاس ورڈ حاصل کر لے تو وہ آپ کی ای میل میں داخل ہونے کے لیے اس کو استعمال نہیں کر سکے گا۔

یاد رکھیں کہ آپ کی ای میل آپ کے سب سے اہم اکاؤنٹس میں سے ایک ہے۔ اس بات کو یقینی بنائیں کہ یہ محفوظ ہو۔

اپنی ای میل کا پاس ورڈ کس طرح تبدیل کریں؟

اپنی جی میل کا پاس ورڈ کس طرح تبدیل کریں:

- جی میل۔
- یاہو!۔
- آؤٹ لک۔
- بی ٹی۔
- اے او ایل ای میل۔

اگر آپ کی ای میل یہاں پر درج نہ ہو تو آپ کو اپنے فراہم کنندہ کا آن لائن مشورہ تلاش کرنا چاہئے کہ آپ اپنی ای میل کا پاس ورڈ کیسے تبدیل کریں۔

پاس ورڈز کے بارے میں سول ٹریڈرز اور چھوٹے کاروبار والوں کے لئے مشورہ

اگر آپ کاروبار کے مالک ہیں تو آپ کے اکاؤنٹس میں آپ کے صارفین، آپ کے کاروبار یا آپ کے مالی معاملات کے بارے میں حساس معلومات شامل ہو سکتی ہیں۔

اگر آپ کے اکاؤنٹس محفوظ نہ ہوں تو آپ کے کاروبار میں سائبر واقعے کا خطرہ زیادہ ہو سکتا ہے۔ اس سے آپ کا کاروبار قانونی یا مالی خطرے سے دوچار ہو سکتا ہے اور جنرل ڈیٹا پروٹیکشن ریگولیشن (جی ڈی پی آر) کے بارے میں عدم تعمیل کا خطرہ لاحق ہو سکتا ہے۔

اگر آپ کے پاس کاروباری عملہ موجود ہو تو آپ کو یہ بات یقینی بنانی چاہئے کہ وہ پاس ورڈ کو اپنے آلات کے قریب محفوظ نہ کریں اور جب آلات زیر استعمال نہ ہوں تو ان کو مقفل یا بند کر دیا جائے۔

مزید معلومات کے لئے نیشنل سائبر سیکیورٹی سینٹر کا چھوٹے کاروبار کا رہنما کتابچہ ملاحظہ فرمائیں۔

تمام مذکورہ لنکس تک رسائی نیشنل سائبر سیکیورٹی سینٹر کی یہ ویب سائٹ وزٹ کر کے حاصل کی جا سکتی ہے https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 2]

[Start Community Language Document 3]

اقدام 2 تین بے ترتیب الفاظ استعمال کر کے مضبوط پاس ورڈز بنائیں

اگر آپ اپنے اہم اکاؤنٹس کیلئے مختلف پاس ورڈز استعمال کرتے ہوں تو ان سب کو یاد رکھنا مشکل ہو سکتا ہے۔

ایک مضبوط اور یادگار پاس ورڈ بنانے کا اچھا طریقہ یہ ہے کہ تین بے ترتیب الفاظ استعمال کیے جائیں۔

ایسے الفاظ استعمال نہ کریں جن سے اندازہ لگایا جا سکتا ہو (جیسا کہ آپ کے پالتو جانور کا نام)۔ اگر ضرورت ہو تو آپ ہندسے اور علامات شامل کر سکتے/سکتی ہیں۔ مثال کے طور پر: RedPantsTree4!

اپنے پاس ورڈز کو اپنے براؤزر میں محفوظ کرنے سے آپ کو ان کا بندوبست کرنے میں مدد ملے گی، ہم اگلی تحریر میں اس کا تفصیل کے ساتھ جائزہ لیں گے۔

ایک مضبوط پاس ورڈ بنانے کے لئے اپنی سوجھ بوجھ کو آزمائیں

کیا آپ اندازہ لگا سکتے/سکتی ہیں کہ ان میں سے کون سا پاس ورڈ سب سے زیادہ 100،000 کمزور پاس ورڈز میں شامل نہیں ہے؟

- arsenal22
- 1v&upjw3nt
- p@55w0rd
- RedPantsTree
- Victoria!

2011977

جواب ہے RedPantsTree

ہیکرز ملین کی تعداد میں کمزور پاس ورڈز پر مشتمل آن لائن فہرستیں شیئر کرتے ہیں۔

3 بے ترتیب الفاظ نئے پاس ورڈ تخلیق کرنے کا ایک آسان طریقہ ہے، آپ کے لیے ان کے منفرد ہونے کا امکان ہوتا ہے اور ان کے بارے میں اندازلگانے کا امکان بھی کم ہوتا ہے۔

تمام مذکورہ لنکس تک رسائی نیشنل سائبر سیکیورٹی سینٹر کی یہ ویب سائٹ وزٹ کر کے حاصل کی جا سکتی ہے۔

https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 3]

[Start Community Language Document 4]

اقدام 3 اپنے پاس ورڈز کو اپنے براؤزر میں محفوظ کر لیں

اپنے پاس ورڈز کو اپنے براؤزر میں محفوظ کرنے کا مطلب یہ ہے کہ آپ کے ویب براؤزر (جیسا کہ کروم، سفاری یا ایج) آپ کے لیے آپ کے پاس وروڈز کو یاد رکھتے ہیں۔

یہ اس میں مدد کر سکتا ہے:

- اس بات کو یقینی بنانا کہ آپ اپنے پاس ورڈز کو گم نہ کر دیں یا بھول نہ جائیں۔
- سائبر جرائم مثلاً "جعلی ویب سائیٹس سے آپ کو محفوظ رکھیں۔

یہ کوئی کمزور پاس ورڈ استعمال کرنے یا ایک ہی پاس ورڈ کو ایک سے زیادہ جگہوں پر استعمال کرنے سے زیادہ محفوظ ہے۔

اس بات کو یقینی بنائیں کہ اگر آپ کا ڈیوائس گم ہو یا چوری ہو جائے تو آپ اپنے محفوظ کردہ پاس ورڈز کی حفاظت کر سکیں۔

اپنے محفوظ کردہ پاس ورڈز کی حفاظت کیسے کریں

آپ کے اکاؤنٹس تک رسائی حاصل کرنے کے لیے آپ کے ڈیوائس تک رسائی حاصل کر لینے والا کوئی بھی شخص آپ کے محفوظ کردہ پاس ورڈز استعمال کر سکتا ہے۔

دور دراز سے انٹرنیٹ پر حملوں کے مقابلے میں جہاں مخصوص سافٹ ویئر کے استعمال کے ذریعے پاس ورڈز کو توڑا جاتا ہے اس قسم کا سائبر کرائم کم عام ہوتا ہے۔

اس بات کو یقینی بنانے کے لئے کہ آپ محفوظ ہوں آپ کو یہ کام کرنے چاہیں:

- جب آپ اپنا ڈیوائس استعمال نہ کر رہے ہوں تو اس کو بند یا مقفل کر دیں۔
- اپنے ڈیوائس کو محفوظ رکھنے کے لیے ایک مضبوط پاس ورڈ استعمال کریں۔
- اپنے تمام آلات اور اکاؤنٹس کے لیے دو عنصر کی توثیق آن کر دیں۔
- اگر آپ کا ڈیوائس اس بات کی اجازت دیتا ہو تو بایومیٹرکس (فیس آئی ڈی یا فنگر پرنٹ شناخت) آن کر دیں۔

آپ کو اپنا ڈیٹا بھی باقاعدگی سے بیک اپ کر لینا چاہئے۔ اگر آپ کا ڈیوائس گم یا چوری ہو جائے تو یہ آپ کو اپنی اہم معلومات کو بازیاب کرنے میں مدد فراہم کرے گا۔

اپنے براؤزر میں اپنے پاس ورڈز کو کیسے محفوظ کریں اپنے پاس ورڈز کو اس میں محفوظ کرنے کا طریقہ معلوم کریں:

- گوگل کروم۔
- مائیکروسافٹ ایج۔
- فائر فاکس۔
- سفاری۔

کیا آپ کو معلوم ہے؟

آپ اپنے محفوظ کردہ پاس ورڈز کو ایک ہی براؤزر سے کسی بھی ڈیوائس پر سائن ان کر سکتے ہیں۔

اضافی تحفظ شامل کریں

ایک بار جب آپ اپنے تمام آلات اور سروسز کے لیے مضبوط اور منفرد پاس ورڈز (اقدامات 1تا3) مرتب کر لیں تو آپ ہیک ہو جانے کے خطرے کو کم کرنے کے لیے دیگر اقدامات بھی بروئے کار لا سکتے/سکتی ہیں (اقدامات 4تا6)۔

تمام مذکورہ لنکس تک رسائی نیشنل سائبر سیکیورٹی سینٹر کی یہ ویب سائٹ وزٹ کر کے حاصل کی جا سکتی ہے۔

https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 4]

[Start Community Language Document 5]

اقدام4دو عنصر کی توثیق(2ایف اے)آن کر دیں

ہیکرز کے پاس خواہ آپ کا پاس ورڈ موجود ہی کیوں نہ ہو دو عنصر کی تصدیق(2ایف اے)انہیں آپ کے اکاؤنٹ میں داخل ہونے سے روکنے میں مدد دیتی ہے۔

چند ایک آن لائن بینکنگ خود کار 2ایف اے کا استعمال کرتی ہیں۔ آپ کی شناخت کی تصدیق کرنے کے لئے یہ مزید معلومات طلب کرتے ہیں جیسا آپ کے فون پر کوڈ بھیجنا۔

دو عنصر کی توثیق(2ایف اے) کس طرح آن کریں

آپ کو اپنے بیشتر اکاؤنٹس کے لیے 2ایف اے آن کرنا ہو گا۔ تمام اکاؤنٹس 2ایف اے پیش نہیں کرتے۔آن لائن بینکنگ خود کار 2ایف اے استعمال کرتی ہیں۔

2ایف اے کو دو مرحلہ جاتی تصدیق یا کثیر الاعناصر توثیق کے نام سے بھی جانا جاتا ہے۔

ویڈیو: 2ایف اے کس طرح کام کرتا ہے

یوٹیوب پر 2ایف اے کس طرح کام کرتا ہے کے بارے میں ویڈیو دستیاب ہے۔

ای میل کے لیے 2ایف اے آن کریں

- جی میل۔
- یاہو!۔
- آؤٹ لک۔
- اے او ایل۔

سوشل میڈیا کے لیے 2ایف اے آن کریں

- انسٹا گرام۔
- فیس بک۔
- ٹویٹر۔
- لینکڈ اِن۔

تمام مذکورہ لنکس تک رسائی نیشنل سائبر سیکیورٹی سینٹر کی ویب سائٹ ویزٹ کر کے حاصل کی جاسکتی ہے

https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 5]

[Start Community Language Document 6]

کاروائی 5 : اپنی ڈیوائس اپ ڈیٹ کریں

پرانے سافٹ ویئر، ایپس اور آپریٹنگ سسٹم میں کمزوریاں موجود ہوتی ہیں۔ اس سے انہیں ہیک کرنا آسان ہو جاتا ہے۔

کمپنیاں اپ ڈیٹ جاری کر کے ان کمزوریوں کو دور کرتی ہیں۔ جب آپ اپنے آلات اور سافٹ ویئر کو اپ ڈیٹ کر لیتے ہیں تو اس سے ہیکرز کو دور رکھنے میں مدد ملتی ہے۔

اپنے آلات اور سافٹ ویئر کیلئے پیش کردہ خودکار اپ ڈیٹس کو آن کر دیں۔ اس کا مطلب یہ ہو گا کہ آپ کو خود یہ کام کرنا یاد رکھنے کی ضروری نہیں ہو گی۔

چند ایک آلات اور سافٹ ویئر کو ہاتھ سے اپ ڈیٹ کرنے کی ضرورت ہوتی ہے۔ آپ اپنے فون یا کمپیوٹر پر یاددہانی حاصل کر سکتے/سکتی ہیں۔ ان یاددہانیوں کو نظرانداز نہ کریں۔ اپ ڈیٹ کرنے سے خود کو آن لائن محفوظ رکھنے میں مدد ملے گی۔

خودکار طریقے سے اپ ڈیٹس چالو کرنے کا طریقہ

معلوم کریں کہ خودکار طریقے سے کس طرح اپ ڈیٹس کو چالو کرنا ہے:

- ایپل-میک
- ایپل-آئی فون اور آئی پیڈ
- مائیکروسافٹ ونڈوز 10۔ اپ ڈیٹس کے لیے ونڈوز 10 تلاش کریں
- اس وقت ونڈوز 7 کے لیے تعاون میسر نہیں ہے۔ آپ کو ونڈوز 10 میں اپ گریڈ کرنا چاہیے۔
- اینڈرائیڈ سمارٹ فون اور ٹیبلیٹس
- اینڈرائیڈ ایپس

سوال: کمپنیاں اپنے سافٹ ویئر میں کمزوریوں کو کس طرح درست کرتی ہیں؟

- بینڈیج
- پیچ
- ریپیئر (مرمتی)

جواب: جب کسی کمپنی کو اپنے سافٹ ویئر میں کوئی کمزوری دکھائی دیتی ہے تو وہ اسے ٹھیک کرنے کے لئے 'پیچ' جاری کرتے ہیں۔ اس سے آپ کی معلومات کو محفوظ رکھنے میں مدد ملتی ہے۔

تمام مذکورہ لنکس تک رسائی نیشنل سائبر سیکیورٹی سینٹر کی یہ ویب سائٹ ویزٹ کر کے حاصل کی جاسکتی ہے۔

https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 6]

[Start Community Language Document 7]

اقدام 6-اپنے ڈیٹا کا بیک اپ بنائیں

بیک اپ کا مطلب اپنی معلومات کی نقل تیار کرنا اور اسے کسی دوسرے ڈیوائس یا کلاؤڈ اسٹوریج میں آن لائن بچا کر رکھنا ہے۔

باقاعدگی سے بیک اپ لینے کا مطلب ہے کہ آپ کے پاس ہمیشہ اپنی معلومات کا حالیہ نسخہ محفوظ ہوگا۔ اگر آپ کا ڈیٹا گم یا چوری ہو جائے تو یہ آپ کو اپنی اہم معلومات بازیاب کرنے میں مدد فراہم کرے گا۔

آپ خودکار بیک اپ بھی چلا سکتے ہیں۔ یہ آپ کے یاد رکھے بغیر آپ کی معلومات کو باقاعدگی سے کلاؤڈ اسٹوریج میں محفوظ کرے گا۔

اگر آپ اپنی معلومات کو کسی یو ایس بی اسٹک یا بیرونی ہارڈ ڈرائیو پر بیک اپ کریں تو جب بیک اپ نہ ہو رہا ہو تو اسے اپنے کمپیوٹر سے منقطع کر دیں۔

کیا آپ کو معلوم ہے؟

آپ کو اپنا ڈیوائس اپ ڈیٹ کرنے سے قبل اپنا ڈیٹا ہمیشہ بیک اپ کر لینا چاہئے۔ اس کی وجہ یہ ہے کہ بعض اوقات اپ ڈیٹ فائلوں کو ختم یا تبدیل کر سکتے ہیں۔

خودکار طریقے سے بیک اپ کو کس طرح چالو کیا جائے

ذیل کے لیے خودکار طریقے سے بیک اپ کو کس طرح چالو کیا جائے:

- ایپل—میک۔
- ایپل-آئی فون اور آئی پیڈ۔
- اینڈرائیڈ۔
- ون ڈرائیو پر مائیکروسافٹ ونڈوز 10 اور ونڈوز 8۔

بیک اپ کے بارے میں سول ٹریڈرز اور چھوٹے کاروبار والوں کے لئے مشورہ

اپنے ڈیٹا کو بیک اپ کر لینے کا مطلب یہ ہوگا کہ اگر کوئی سائبر واقعہ پیش آجاتا ہے تو آپ کا کاروبار چلتا رہے۔

اپنے کاروبار کے بارے میں سب سے اہم اعداد و شمار کی نشاندہی کرنے سے آغاز کریں۔ ان میں مالیات، معاہدے، کسٹمر یا اسپلائر کے بارے میں معلومات شامل ہو سکتی ہیں۔ اس بات کو یقینی بنائیں کہ اس کا باقاعدگی سے بیک اپ لیا جائے۔

آپ کو یہ بھی جاننا چاہئے کہ ڈیٹا ضائع ہونے کی صورت میں بیک اپ کو کیسے بحال کرنا ہے۔

مزید معلومات کے لئے نیشنل سائبر سیکیورٹی سینٹر کا چھوٹے کاروبار کار ہنما کتابچہ ملاحظہ فرمائیں۔

تمام مذکورہ لنکس تک رسائی نیشنل سائبر سیکیورٹی سینٹر کی یہ ویب سائٹ ویزٹ کر کے حاصل کی جاسکتی ہے۔

https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document7]

[END OF DOCUMENT]