BritishRedCross

Home Office

رفیوجی ویمین ڈیجیٹل امپاورمنٹ اینڈ کنیکٹ پروجیکٹ

ورکشاپ 3 کا ساتھ دینے کے لیے ہدایت نامہ

یہ ہدایت نامہ ان عورتوں کے لیے ایک معاونتی ٹول کے طور پر تیار کیا گیا ہے جو ڈیجیٹل رفیوجی ویمین امپاورمنٹ اینڈ کنیکٹ (Digital Refugee Women Empowerment and connect) پروجیکٹ کے ورکشاپس میں شرکت کر رہی ہیں۔ اس کا ہدف وہ عورتیں ہیں جنہیں پناہ گزین کی حیثیت، خادم خلق کا تحفظ یا رفیوجی فیملی ری-یونین حاصل ہے اور جو یوکے میں رہتی ہیں۔ اس پروجیکٹ کو رقم کی فراہمی ہوم آفس رفیوجی اسائلم سپورٹ اینڈ انٹیگریشن (Home Office Resettlement Asylum Support and Integration directorate) فنڈ کے ذریعہ کی جاتی ہے۔

ہم وائس (Voice) کے نیٹ ورک کے ممبران اور وائس کے سفیروں کا شکریہ ادا کرنا چاہیں گے جنہوں نے ان روایتی دستاویزات کی تخلیق میں تعاون کیا ہے۔ مواد انگریزی، امہرک، عربی، فارسی، کردستانی (سورانی)، صومالی، ٹگرینیا اور اردو میں دستیاب ہیں۔ امید کی جاتی ہے کہ وہ پناہ گزین عورتیں جو ورکشاپس میں حصہ نہیں لے سکی تھیں ان کے لیے اس پر ابھی بھی نظر ڈالنا کار آمد ہو سکتا ہے اور وہ اپنی رفتار سے یہاں فراہم کردہ معلومات کا جائزہ لے سکتی ہیں۔

مشمولات

تمہید

یہ ٹول ان تمام دھمکیوں اور تحفظ کی تدابیر کا مکمل جائزہ لینے سے قاصر ہے جو انٹرنیٹ استعمال کنندگان کے لیے دستیاب ہیں لیکن یہ آپ کی توجہ صرف کچھ کلیدی نکات اور ان جگہوں کی طرف مرکوز کرنے کی امید رکھتا ہے جہاں آپ مزید معلومات پا سکتی ہیں۔

ہم اعتراف کرتے ہیں کہ ڈیجیٹل تحفظ کے بارے میں بات کرتے وقت ہم جنس پر مبنی تشدد (Gender Based Violence)، بدسلوکی اور قابل تعزیر جرائم سے متعلق مسائل پر بات کرتے ہیں، جو حساس اور اکثر ممنوع ہو سکتا ہے۔ ہمارے خادم خلق مشن اور نقصان نہ پہنچاؤ کے اصول کا مطلب ہے کہ جنس پر مبنی تشدد کے مسئلہ کو سلجھانے کی خاطر ہمیں وہ کارروائی کرنے کے لیے بلایا جاتا ہے جو ہمارے اختیار میں ہے، جس میں ایسے انتخابات کرنے کی خاطر لوگوں کا تعاون کرنے کے لیے معلومات فراہم کرنا بھی شامل ہے جو انہیں اختیار فراہم کرتے ہیں اور ایسے فیصلے کرنے میں بھی جو انہیں تحفظ فراہم کرتے ہیں۔

اس پورے ہدایت نامہ میں آپ متن کے اندر داخل کردہ لنک پائیں گی، جن پر اگر آپ کلک کریں گی تو وہ آپ کو مذکورہ ویب سائٹ تک لے جائیں گی۔ مثال کے طور پر، اگر آپ یہاں پر کلک کریں گی تو آپ برٹش ریڈ کراس (British Red Cross) کی ویب سائٹ تک لے جائی جائیں گی۔ جہاں ممکن رہا ہے، ہم نے ترجمہ شدہ ذرائع کے لنکس شامل کرنے کی کوشش کی ہے، لیکن اس ہدایت نامہ میں بہت سے لنکس ان معلومات کے لیے ہیں جو انگریزی میں ہیں۔ اگرچہ ہم خودکار ترجمہ کی حدود کا اعتراف کرتے ہیں، تاہم ہم نے اس بارے میں معلومات فراہم کر دی ہیں کہ اس فنکشن کا استعمال ہدایت نامہ دو میں کس طرح کریں۔

ڈیجیٹل تحفظ بشمول اس بارے میں کہ اپنے آلات کی حفاظت کس طرح کریں، اور خود کو اور دوسروں کو آن لائن دھمکیوں سے محفوظ رکھنے کے اقدامات سے متعلق جامع صلاح www.getsafeonline.org.uk اور نیشنل سائبر سیکورٹی سنٹر (National Cyber Security Centre) www.ncsc.gov.uk کی طرف سے دستیاب ہے۔ آن لائن بدسلوکی کے شکار افراد کے لیے مزید معلومات اور تعاون اسٹاپ آن لائن ابیوز (Stop Online Abuse) – www.stoponlineabuse.org.uk کی طرف سے دستیاب ہیں۔ کسی بھی قسم کے جنس پر مبنی تشدد، گھریلو بدسلوکی یا ہراسانی کو سلجھانے یا اس کی اطلاع دینے کی خاطر مزید معلومات یا تعاون کے لیے رفیوج (Refuge) یا نیشنل ڈومیسٹک ابیوز ہیلپ لائن (National Domestic Abuse Helpline) / www.refuge.org.uk www.nationaldahelpline.org.uk 0808 2000 247 پر رابطہ کریں۔

اگر آپ کو فوری تشویشات لاحق ہیں یا آپ کسی جرم کی اطلاع دینا چاہتی ہیں تو پولیس سے رابطہ کریں – 999 (ایمرجنسی) – 101 (غیر ایمرجنسی)

کلیدی اصطلاحات

ڈیجیٹل تحفظ - انٹرنیٹ استعمال کرتے وقت خود کو، دوسروں کو اور اپنی ذاتی معلومات کو محفوظ رکھنے کے لیے اعمال اور عادتیں

باہمی - لوگوں کے مابین تعاملات سے متعلق

آن لائن دھمکی - کوئی ایسا خطرہ یا پریشانی جو انٹرنیٹ کے واسطہ سے کسی ان چاہے واقعہ یا عمل کا باعث بنتی ہے

پاسورڈ - حروف کا ایک خفیہ سلسلہ جو کسی کمپیوٹر سسٹم یا خدمت تک رسائی فراہم کرتا ہے

مامون - محفوظ اور بے خوف و خطر رہنا، خطرے یا نقصان کی زد میں نہ آنا۔

ڈیجیٹل تحفظ کیا ہے؟

ڈیجیٹل تحفظ کا مطلب خود کو (اور اپنے ڈیٹا کو) آن لائن خطرات سے محفوظ رکھنے کے بارے میں آگاہ ہونا اور جاننا ہے۔ اکثر ڈیجیٹل تحفظ کا مطلب بس کچھ ایسی اچھی عادتوں کا حامل ہونا ہے جو آپ کو سائبر-کرائم، دھوکے، یا دھمکیوں کے

تئیں کم ضرر پذیر بناتی ہیں۔ اس میں کچھ ایسی چالوں کا جاننا بھی شامل ہے جنہیں مجرم افراد لوگوں کو انہیں معلومات یا پیسے حوالے کرنے، یا آپ کی نجی زندگی میں بے جا مداخلت کرنے کے لیے، استعمال کر سکتے ہیں۔

آن لائن دھمکی کی سب سے زیادہ عام قسمیں درج ذیل سے سامنے آتی ہیں

- ایسے وائرسیز اور میلویئر جو آپ کی ذاتی معلومات یا اکاؤنٹ کی تفصیلات چرانے ("ہیک کرنے")، یا ایسے پروگرام نصب کرنے کی کوشش کرتے ہیں جو آپ پر نظر رکھ سکتے ہیں
- آن لائن دھوکہ دہی جس میں مجرم افراد آپ کو معلومات حوالے کرنے کے لیے قائل کرنے کی کوشش کرتے ہیں
- ایسے دھونس جمانے والے، تعاقب کرنے والے اور بدسلوکی کرنے والے افراد جو آپ کو ہراساں کرنے، آپ کے ساتھ بدسلوکی کرنے یا آپ کو کنٹرول کرنے کے لیے آن لائن گمنامی کا فائدہ اٹھاتے ہیں۔

آن لائن دھمکیاں مالی، جذباتی، اور ذاتی سلامتی کو متاثر کرنے کی صلاحیت رکھتی ہیں۔ اہم بات یہ ہے کہ اس میزان کو ذہن میں رکھتے ہوئے ڈیجیٹل تحفظ سے متعلق آگاہی لوگوں کو آن لائن اپنا اعتماد بڑھانے میں مدد دیتی ہے۔

ڈیجیٹل تحفظ سے متعلق ضروری سفارشات

مضبوط پاسورڈز رکھنا

ای میل اور آن لائن تمام دیگر اکاؤنٹس ایک پاسورڈ اور ایک کلید کے ذریعہ مقفل کیے جاتے ہیں، تاکہ دوسروں کو آپ کے اکاؤنٹ تک رسائی حاصل کرنے سے روکا جا سکے۔ پاسورڈ کو پیچیدہ یا "مضبوط" رکھنا کسی کو آپ کی نجی معلومات تک پہنچنے سے روکنے کا سب سے بہترین طریقہ ہے۔

ایک مضبوط ای میل پاسورڈ رکھنا ضروری ہے۔ اگر کوئی ہیکر آپ کے ای میل تک پہنچ جاتا ہے تو وہ 'forgot password' ('پاسورڈ بھول گئے') فیچر کا استعمال کرتے ہوئے آپ کے تمام دیگر اکاؤنٹس کے پاسورڈز دوبارہ مرتب کر سکتا ہے اور آپ کے تمام اکاؤنٹس میں موجود حساس ذاتی معلومات تک رسائی حاصل کر سکتا ہے۔

ہیکرز جانتے ہیں کہ ہم میں سے بہت سے لوگ 123456، اپنی زندگیوں کی کوئی اہم تاریخ یا بچہ کے نام جیسے پاسورڈز کا انتخاب کرتے ہیں – کوئی ایسی چیز استعمال کرنے پر آمادہ نہ ہوں جس کا آسانی سے اندازہ لگایا جا سکے۔ آسان پاسورڈز جلدی توڑے جا سکتے ہیں، لیکن ایک اچھا پاسورڈ مجرموں کو باہر ہی مقفل رکھتا ہے۔ کوئی پاسورڈ تیار کرنے کے لیے وقت نکالنا اہم ہے۔

کوئی نیا مضبوط پاسورڈ تخلیق کرنے کے لیے ان مراحل پر عمل کریں:

1. تین بے ترتیب الفاظ کو ملائیں: مثلاً rugfirefork کو بنانے کے لیے rug، fire، fork۔
2. اپرکیس لیٹرز شامل کریں، مثلاً RugFireForK
3. نمبرات شامل کریں، مثلاً 19RugFireForK90، اور
4. پاسورڈ کو مزید پیچیدہ بنانے کے لیے علامات شامل کریں: !19RugFireForK90

ہیکرز لاکھوں شناخت شدہ پاسورڈز کی فہرستیں شیئر کرتے ہیں اور تین بے ترتیب الفاظ ایسے نئے پاسورڈز تخلیق کرنے کا زیادہ آسان طریقہ ہے جس کا آپ کے لیے منفرد ہونے کا امکان زیادہ ہے اور جس کا اندازہ لگائے جانے کا امکان کم ہے۔ تاکید کے ساتھ صلاح دی جاتی ہے کہ آپ وقت وقت سے اپنے پاسورڈز تبدیل کرتے رہیں اور اپنے تمام اکاؤنٹس کے لیے ایک ہی پاسورڈ نہ استعمال کریں۔ اگر آپ کو نئے پاسورڈز تیار کرنے میں دشواری ہوتی ہے تو پاسورڈ جنریٹر بھی ایک اچھا انتخاب ہے۔

کوئی پاسورڈ منیجر استعمال کریں

اگر آپ فکرمند ہیں کہ آپ کو 'مضبوط' پاسورڈز یاد نہیں رہیں گے تو آپ کسی پاسورڈ منیجر کا استعمال کر سکتی ہیں۔ پاسورڈ منیجرز کا مطلب ہو سکتا ہے اپنا پاسورڈ ویب براؤزر (جیسے گوگل کروم (Google Chrome) یا مائیکروسافٹ ایج (Microsoft Edge)) میں محفوظ کرنا، تاکہ براؤزر آپ کے لیے پاسورڈ کو یاد رکھے۔ وہ خراب یا کمزور پاسورڈز استعمال کرنے سے زیادہ محفوظ ہیں لیکن انہیں محفوظ رکھنا نہ بھولیں تاکہ آپ کا آلہ کھو جانے کی صورت میں کام آئے۔ اینٹی وائرس اور آن لائن تحفظ میں خصوصی مہارت رکھنے والی کچھ کمپنیاں معیار کے طور پر ایک پاسورڈ منیجر فراہم کریں گی، اگر آپ ان کے اینٹی وائرس ٹولز خریدیں گی؛ کچھ دیگر کمپنیاں خود ہی پاسورڈ منیجرز فراہم کریں گی۔

دو عنصر والی توثیق مرتب کریں

دو عنصر والی توثیق آپ کے پاسورڈ کے علاوہ مزید ایک عدد معلومات طلب کرتے ہوئے آپ کے اکاؤنٹ میں تحفظ کی ایک دوسری پرت کا اضافہ کرتی ہے۔ یہ دوسروں کو آپ کے اکاؤنٹس تک پہنچنے سے روکنے میں مدد دیتی ہے، خواہ ان کے پاس آپ کا پاسورڈ بھی ہو۔ معروف ای میل اور سوشل میڈیا کے لیے دو عنصر والی توثیق کس طرح چالو کریں اس بارے میں رہنمائی **نیشنل سائبر سیکورٹی سنٹر** کی ویب سائٹ پر یہاں مل سکتی ہے۔

اپنے آلات کو وائرسیز سے محفوظ رکھنا

وائرسیز وہ خفیہ پروگرامز ہیں جن کی ترسیل ویب سائٹوں، ای میل کے لنکس، منسلکات یا علیحدہ کیے جانے کے قابل میڈیا (جیسے USB اسٹکس) کے ذریعہ کی جاتی ہے۔ وہ بہت زیادہ خلل کا باعث بن سکتے ہیں اور آپ کو آپ کے کمپیوٹر یا اکاؤنٹس کے باہر مقفل کر سکتے ہیں، فروخت یا استعمال کرنے کے لیے ذاتی معلومات یا ڈیٹا چرا سکتے ہیں، آپ کے پیسے لے سکتے ہیں یا آپ کے گھر میں آپ پر نظر بھی رکھ سکتے ہیں۔ فکر کی بات یہ ہے کہ ہر کوئی یہ نہیں جانتا ہے کہ اپنے آلات کو ان خطرات سے کس طرح محفوظ رکھیں، یا انہیں محفوظ رکھنے کے لیے کون سے اقدامات کریں۔ ONS نے رپورٹ دی ہے کہ 2020 میں، ان بالغان میں سے جن کے پاس اسمارٹ فون ہیں، 17% لوگوں نے اپنے اسمارٹ فون میں سیکورٹی نہیں رکھی تھی اور 32% لوگ نہیں جانتے تھے کہ انہیں سیکورٹی حاصل تھی یا نہیں۔

کسی سیکورٹی گارڈ کی طرح، **اینٹی-وائرس** لیپ ٹاپ، ٹیبلیٹ یا فون پر نصب کیا جانے والا ایک ایسا ٹول ہے جو ان پریشانی کا باعث بننے والے پروگراموں کو آپ کے آلات کو متاثر کرنے سے روکتا ہے۔ کسی کمپیوٹر، لیپ ٹاپ، ٹیبلیٹ یا اسمارٹ فون کے لیے **اینٹی**-وائرس کا تحفظ ان جیسے عام خطرات کو روکنے میں مدد کرنے کے لیے اہم ہے:

- **ٹروجنس (Trojans)** جو ایسا پروگرام ہونے کا بہانہ کرتے ہیں جنہیں آپ ڈاؤن لوڈ کرنا چاہتی ہیں (جیسے کوئی **اینٹی**-وائرس پروگرام، کوئی فوٹو یا کوئی مفت فلم) لیکن پرعناد سافٹ ویئر (میلویئر) ہوتے ہیں یا اس پر مشتمل ہوتے ہیں جو اس وقت سرگرم ہو جاتے ہیں جب آپ اسے کسی کمپیوٹر یا فون پر نصب کرتی ہیں۔
- **اسپائی ویئر (Spyware)** جو مجرمانہ مقاصد کے لیے معلومات کا پتہ لگاتے اور ان چیزوں پر نظر رکھتے ہیں جو آپ اپنے پی سی پر کر رہی ہوتی ہیں۔
- **ایڈویئر (Adware)** جو ایسے پوپ-اپ ونڈوز کھولتے ہیں جو آپ کے ہاتھوں چیزیں فروخت کرنے کی کوشش کرتے ہیں۔
- **رینسم ویئر (Ransomware)** جو آپ کو آپ کے آلہ کے باہر مقفل کر دیتا ہے اور ادائیگی کا مطالبہ کرتا ہے۔
- **اسپیم (Spam)** ایسے پروگرامز تیار کرتا ہے جنہیں وارمز کہا جاتا ہے، جو کھلے ہوئے ویب کنیکشنز کے ذریعہ آپ کے سسٹم میں گھس جاتے ہیں اور پھر آپ کے رابطوں کو بہت سے ان چاہے "اسپیم" ای میلز بھیجنے کے لیے نقل تیار کرتے ہیں۔ ان چاہی ای میل مواصلات کو **اسپیم** یا **جنک ای میل** کے نام سے جانا جاتا ہے۔ اسپیم ای میل بس زحمت کا باعث ہو سکتے ہیں، لیکن یہ لوگوں کو دھوکے سے نقصان پہنچانے اور غلط معلومات پھیلانے کے لیے بھی استعمال کیے جا سکتے ہیں۔

زیادہ تر سسٹمز میں پہلے ہی سے کچھ **اینٹی-وائرس یا اسپائی ویئر تحفظ** نصب ہوں گے، مثال کے طور پر مائیکروسافٹ ونڈوز 10 (Microsoft Windows10) والے لیپ ٹاپس میں پہلے ہی سے ونڈوز ڈفینڈر (Windows Defender) نصب ہوں گے۔

آپ اضافی اینٹی-وائرس تحفظ حاصل کر سکتے ہیں: کبھی کبھی یہ مفت ہوتا ہے، لیکن ایسی کمپنیاں بھی ہیں جو بامعاوضہ پروگرامز فراہم کرتی ہیں۔

زیادہ پرانے سافٹ ویئر میں ایسے ہول (سوراخ) ہو سکتے ہیں جن سے وارسیز اندر گھس سکتے ہیں۔ **اپڈیٹس** ان ہول پر پیچ لگانے کا موقع دیتے ہیں۔ آپ سیکورٹی میں کسی بھی ہول پر پیچ لگانے کی خاطر خودکار طور پر اپڈیٹ کرنے کے لیے پروگراموں اور سافٹ ویئر کا انتظام کر سکتی ہیں۔ اس کا مطلب یہ ہے کہ آپ کے لیے ایسا کرنے کے لیے یاد رکھنا ضروری نہیں ہے۔ کبھی کبھی آپ کو آلہ کو دستی طور پر اپڈیٹ کرنے کی ضرورت ہو سکتی ہے اور اگر ایسی صورت ہے تو آپ کو عام طور پر ایک یاددہانی موصول ہوگی۔ انہیں نظر انداز نہ کریں!

اپنے ڈیٹا کا بیک اپ رکھیں

وائرسیز آپ کے ڈیٹا اور معلومات کو حذف کر سکتے ہیں یا انہیں چرا سکتے ہیں۔ اپنی ذاتی تصاویر، فائلوں اور معلومات کو محفوظ رکھنے کے لیے آپ کو اپنا آلہ اپڈیٹ کرنے سے پہلے ڈیٹا کا بیک اپ رکھنا چاہیے۔ بیک اپ کا مطلب ہے ایک نقل تیار کرنا، جو کوئی قابل انتقال ہارڈ ڈرائیو استعمال کرتے ہوئے طبیعی ہو سکتا ہے، لیکن زیادہ تر دوسرے آلہ میں یا "کلاؤڈ" (cloud) (آن لائن) اسٹوریج میں منتقل کرنا ہوتا ہے۔ ایسا اس لیے ہے کیوں کہ کبھی کبھی اپڈیٹس سے فائلیں بدل سکتی ہیں، اگر آپ کے پاس اپنے ڈیٹا کے ایسے بیک اپس ہیں جنہیں آپ جلدی سے بحال کر سکتی ہیں تو رینسم ویئر کے حملوں کے ذریعہ آپ کو بلیک میل نہیں کیا جا سکتا۔ آپ خودکار بیک اپ چالو کر سکتی ہیں جس کا مطلب یہ ہے کہ آپ کو اپنے ڈیٹا کا بیک اپ رکھنے کے لیے یاد رکھنے کی ضرورت نہیں ہے۔

اپنے ڈیٹا کا بیک اپ رکھنے سے متعلق مزید رہنمائی یہاں مل سکتی ہے www.getsafeonline.org/protecting-your-computer/Backups

خلاصۂ کلام

- صرف اپنے ای میل کے لیے ایک علیحدہ پاسورڈ رکھیں
- جانچ کریں کہ آپ کے ای میل کا پاسورڈ اور دیگر اکاؤنٹ کے پاسورڈز مضبوط ہیں
- جانچ کریں کہ آپ اپنا پاسورڈ تبدیل کرنا جانتی ہیں اور ایسا برابر کریں
- کئی اکاؤنٹس کے لیے ایک ہی پاسورڈ نہ استعمال کریں اور اگر آپ پاسورڈز بھول جانے کے بارے میں فکرمند ہیں تو ایک پاسورڈ منیجر استعمال کرنے پر غور کریں
- دو عنصر والی توثیق کا استعمال کریں
- جانچ کریں کہ آپ کے پاس اینٹی-وائرس ہے اور یہ کہ یہ چالو ہے (اور اگر آپ کو یقین نہ ہو تو ایک حاصل کریں)
- اپنا اینٹی-وائرس استعمال کریں اور اسے اپڈیٹ کریں – برابر پورے سسٹم کا اسکین کریں اور نئے تیار کردہ وائرسیز یا بگس کے خلاف تحفظ فراہم کرنے کے لیے اپنے اینٹی-وائرس کو اپڈیٹ کریں
- اس بارے میں دھیان رکھیں کہ آپ کیا ڈاؤن لوڈ کرتی ہیں – اشتہار یا اسپائی ویئر پروگرامز خود کو ان چیزوں سے منسلک کرتے ہوئے آپ کے کمپیوٹر تک پہنچتے ہیں جو آپ ڈاؤن لوڈ کرتی ہیں، اس لیے جانچ کریں کہ آپ اپنی فائلیں کہاں سے وصول کرتی ہیں۔

اگر چیزیں غلط ہو جائیں تو کیا کریں

اگر آپ نے اپنے لیپ ٹاپ میں کوئی لنک کھولا ہے یا کوئی چیز نصب کرنے کے لیے ہدایات کی تعمیل کی ہے لیکن آپ کو شبہ ہے تو اینٹی-وائرس سافٹ ویئر کھولیں اور مکمل اسکین چلائیں۔ اینٹی-وائرس کو انفیکشن تلاش کرنے اور اسے ٹھیک کرنے کا موقع دیں اور جو صلاح وہ دیتا ہے اس پر عمل کرتے ہوئے اپنے آلہ کو بحال کریں۔ اگر یہ ٹھیک نہیں کیا جا سکتا تو آپ کو ماہر کی مدد لینی پڑ سکتی ہے۔

آپ کی قریبی دوست آپ سے رابطہ کرتی ہے اور بہت پریشان معلوم ہوتی ہے۔ انہوں نے ایک ای میل میں ایک فائل کھولی تھی جو ان کے خیال کے مطابق ایک تصویر تھی۔ یہ حقیقت میں ایک ٹروجن ہارس تھا جس میں رینسم ویئر پوشیدہ تھا اور اب وہ اپنے کمپیوٹر کے باہر مقفل ہیں۔ آپ کیا کریں گی، اور آپ انہیں کیا کرنے کے لیے کہیں گی؟

اگر آپ رینسم ویئر سے متاثر ہوئی ہیں تو یاد رکھیں کہ اگر آپ رینسم ادا کرنے کا انتخاب کرتی ہیں تو یہ مجرمانہ سرگرمی کے لیے رقم مہیا کرے گا اور اس کی کوئی ضمانت نہیں ہے کہ آپ اپنے آلہ تک رسائی حاصل کرنے کی اہل ہوں گی؛ ان چاہے طور پر یہ اس طرح کا تاثر دے سکتا ہے کہ آپ مستقبل میں دوبارہ ادائیگی کرنے کے لیے تیار ہیں اور آپ مستقبل میں حملوں کی دعوت دیتی ہیں۔

آن لائن دھمکی کی عام قسمیں

دھوکہ دہی اور اسکیم (فریب)

اسکیم کسی سے رقم اینٹھنے یا اپنی ذاتی تفصیلات فراہم کرنے کے لیے جال میں پھنسانے کی ایک چال ہے، تاکہ ایک مجرم ان کے اکاؤنٹ سے چوری کر سکے یا ان کی شناخت چرا سکے۔ اس میں کسی کے کمپیوٹر یا آن لائن اکاؤنٹ سے ڈیٹا چرانے اور انہیں گمراہ کرتے یا دھوکہ دیتے ہوئے انہیں پیسے حوالے کرنے پر آمادہ کرنے کے لیے وائرسیز کا استعمال کرنا بھی شامل ہو سکتا ہے۔

اسکیم اکثر نقلی ای میل (**فشنگ**)، متنی پیغام (**اسمشنگ**) یا فون کال (**وشنگ**) کا استعمال کرتے ہوئے انجام دیا جاتا ہے۔ ای میلز یا متن میں کسی ایسی نقلی ویب سائٹ کا لنک ہو سکتا ہے جو آپ کو ذاتی معلومات داخل کرنے کے لیے آمادہ کر سکتی ہے یا ایک کوریڈور کے طور پر کام کر سکتی ہے اور وائرسیز کو آپ کے کمپیوٹر میں آنے کا موقع فراہم کرتی ہے۔ یا اس ای میل میں کوئی ایسی منسلکہ چیز ہو سکتی ہے جس میں ایسا وائرس شامل ہو سکتا ہے جو بینکنگ کی تفصیلات، ذاتی معلومات یا تصاویر چراتا ہے۔

اسکیمز آپ کو احساس دلاتے ہیں کہ آپ سے ایک ایسی تنظیم کے ذریعہ رابطہ کیا جا رہا ہے جسے آپ جانتی ہیں یا کسی ایسے شخص کے ذریعہ جسے مدد کی ضرورت ہے۔ وہ اس طرح تیار کیے جاتے ہیں کہ آپ کوئی کام "کرنے" – کوئی لنک کھولنے، تفصیلات فراہم کرنے، کسی منسلکہ چیز پر کلک کرنے کی خاطر کارروائی کرنے کے لیے دباؤ محسوس کریں۔ اس پر یقین نہ کریں!

ہمارے پاس یہاں ہر طرح کے اسکیم اور دھوکہ دہی کی فہرست پیش کرنے کے لیے کافی وقت نہیں ہے۔ اسکیمز کی ان قسموں سے متعلق مزید معلومات جو مجرم استعمال کرتے ہیں، اور اسی طرح اس بارے میں صلاح کہ دھوکہ دہی اور سائبر-کرائمز کی اطلاع کس طرح دیں یہاں مل سکتی ہے: www.actionfraud.police.uk

فشنگ

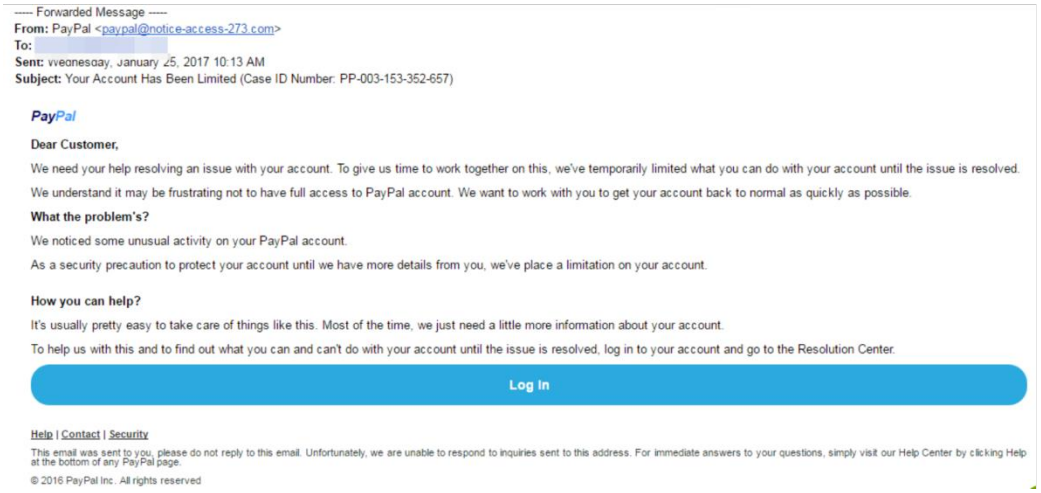
فشنگ اسکیم کی ایک قسم ہے، جس میں کوئی سائبر-کریمنل ذاتی معلومات، بینکنگ یا بینک کارڈ کی تفصیلات، یا اکاؤنٹ کی تفصیلات اور پاسورڈز فراہم کرنے کی خاطر افراد کو ورغلانے کے لیے ایک "ہُک" کا استعمال کرتا ہے۔ پھر وہ اس معلومات کا استعمال آپ کے اکاؤنٹس تک رسائی حاصل کرنے اور آپ سے پیسے یا ای میل کے رابطے چرانے یا آپ کی شناخت چرانے کے لیے کرتے ہیں۔ مجرم اس امید میں ہزاروں لوگوں کو فشنگ ای میل بھیج سکتے ہیں کہ وہ ان میں سے کچھ کو انہیں پیسے یا معلومات حوالے کرنے کے لیے آمادہ کر سکتے ہیں۔

ہیکرز یا اسکیمرز کوئی ایسا شخص یا تنظیم ہونے کا بہانہ کرنے کا شاندار کام کریں گے جس پر آپ بھروسہ کرتے ہیں، اور وہ آپ کو قائل کرنے کے لیے آپ کا نام اور دیگر ذاتی معلومات بھی استعمال کر سکتے ہیں۔ وہ کسی پیش کش کے ذریعہ آپ کو ورغلانے یا کسی دھمکی کے ذریعہ آپ کو چارہ بنانے کی کوشش کریں گے۔ مثال کے طور پر، حکومت کا مثلاً ٹیکس آفس ہونے کا بہانہ کر سکتے ہیں جو آپ سے پیسہ کی واپسی کی پیش کش کرنے کے لیے رابطہ کر رہے ہیں، لیکن یہ کہ انہیں ضرورت ہے کہ آپ کو ادائیگی کرنے کے لیے آپ انہیں اپنی بینک کی تفصیلات فراہم کریں۔ وہ آپ کی مقامی کونسل ہونے کا بہانہ کر سکتے ہیں، یہ کہتے ہوئے کہ آپ کو جرمانہ ادا کرنا ہے، ورنہ آپ کو عدالت جانا پڑے گا، یا آپ کے بینک یا بینکنگ کا ثالث جیسے PayPal ہونے کا بہانہ کر سکتے ہیں اور کہہ سکتے ہیں کہ آپ اپنا بینک اکاؤنٹ استعمال کرنے سے روک دئے گئے ہیں۔

فشنگ پر میٹروپولیٹن پولیس کی جانب سے یہ ویڈیو دیکھیں۔

یہ جانچ کرنے کا ایک فوری طریقہ کہ فی الواقع ای میل کس نے بھیجا ہے اور آیا یہ ایک فشنگ اسکیم ہے ارسال کنندہ کے ای میل پتہ پر نظر ڈالنا ہے، نہ کہ صرف اس پر جو اوپر "From" میں دکھاتا ہے۔ کوئی حقیقی پیغام اکثر کسی قابل شناخت تنظیمی پتہ (مثلاً noreply@yourbank.com) سے آئے گا لیکن اسکیمرز اور مجرمین آپ کے بینک یا تنظیم کے اصل ڈومین نام کا استعمال نہیں کر سکتے، اس لیے اکثر ای میل پتہ بے ترتیب حروف اور نمبرات سے بھرے گئے ہوں گے (مثلاً noreply@1234bank12.com). اگر یہ کسی نجی پتہ (مثلاً person@gmail.com) کی طرف سے ہے تو اس کا امکان بہت کم ہے کہ یہ سرکاری تنظیم کی طرف سے ہوگا – حتی کہ گوگل بھی تنظیمی ای میلز بھیجنے کے لیے GoogleMail (@gmail) ڈومین کا استعمال نہیں کرتا ہے۔

اس مثال پر نظر ڈالتے ہوئے آپ دیکھ سکتی ہیں کہ اگرچہ یہ PayPal کی طرف سے ایک حقیقی ای میل جیسا نظر آتا ہے، تاہم یہ ایک **الگ ڈومین نام** کی طرف سے ہے: Paypal@**notice-accessxxx.com**



----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

ایسے ای میلز سے محتاط رہنا بہتر ہے جو اتنے اچھے معلوم ہوں کہ صحیح نہ لگتے ہوں، یا جو فوری جواب دینے کے لیے آپ پر دباؤ ڈالتے ہوں خواہ وہ صحیح لوگو کا استعمال کریں اور اصل کی طرح نظر آئیں۔ پرسکون رہیں اور پوچھیں کہ آپ کو کیا موصول ہوا ہے۔ جواب نہ دیں یا کسی لنک پر کلک نہ کریں۔ جب آپ کوئی لنک کھولیں گے تو وائرسیز معلومات چرانے کے لیے آپ کے کمپیوٹر پر نصب کیے جا سکتے ہیں، یا آپ کسی پرعناد یا نقلی ویب سائٹ کی طرف بھیجے جا سکتے ہیں اور آپ سے اکاؤنٹ یا بینک کی تفصیلات داخل کرنے کے لیے کہا جا سکتا ہے جو پھر آپ سے چوری کر لی جائیں گی۔

فشنگ اور اسکیم ای میلز کی شناخت کرنا

- کیا آپ ارسال کنندہ کو جانتی ہیں؟ کیا وہ آپ کو عمومی سلام و دعا میں متوجہ کرتے ہیں؟
- کیا اس میں املا کی غلطیاں ہیں یا یہ خراب انداز میں لکھا گیا ہے؟
- کیا یہ آپ سے کوئی کام کرانا چاہتا ہے یا اس میں جلد بازی کا احساس پایا جاتا ہے یا یہ آپ کو دھمکی دیتا ہے؟
- وہ ای میل پتہ کھولیں جس سے پیغام بھیجا گیا ہے۔ کیا اس میں ڈومین کا نام صحیح ہے؟
- یہ غیر متوقع ہے یا کسی ایسی کمپنی کی طرف سے ہے جس کے ساتھ آپ کا کوئی تعلق نہیں ہے؟
- اگر یہ آپ کی رہنمائی کسی ویب سائٹ کی طرف کرتا ہے تو کیا اس ویب سائٹ پر پیڈلاک کا کوئی نشان نہیں ہے اور اس ویب پتہ کے آغاز میں کوئی https:// نہیں پایا جاتا ہے؟

فشنگ ای میلز کی شناخت کرنے سے متعلق مزید معلومات یہاں مل سکتی ہے: www.ncsc.gov.uk

زہرہ کو ایک ای میل موصول ہوتا ہے جس کے بارے میں وہ سمجھتی ہیں کہ وہ ان کے بینک کی طرف سے ہے – اسے کھولنے سے انہیں پتہ چلتا ہے کہ وہ کہتے ہیں کہ انہوں نے ان کا اکاؤنٹ عارضی طور پر موقوف کر دیا ہے۔ مایوسی کی حالت میں، زہرہ کو پتہ چلتا ہے کہ ان کے بینک کو ان کے بینک کھاتہ میں غیر معمولی سرگرمی نظر آئی ہے اور انہوں نے انہیں محفوظ رکھنے کے لیے اسے بند کرنے کا فیصلہ کیا ہے۔ یہ کہتا ہے کہ وہ اس وقت تک بینک کھاتہ نہیں استعمال کر سکتی ہیں جب تک کہ وہ لاگ-ان نہ کریں اور اسے دوبارہ نہ چالو کریں اور یہ ان سے ایک لنک پر کلک کرنے کے لیے کہتا ہے۔ زہرہ جانتی ہیں کہ انہیں کل کرایہ ادا کرنا ہے، اور ان کے لیے اپنے اکاؤنٹ تک رسائی حاصل کرنا ضروری ہے، لیکن وہ شبہ میں ہیں۔

زہرہ صلاح کے لیے آپ کو کال کرتی ہیں: آپ ان سے کیا کہتی ہیں اور آپ انہیں کس طرح صلاح دے سکتی ہیں؟

یہ لنک خطرناک ہو سکتی ہے۔ اس کا مطلب یہ ہو سکتا ہے کہ ہیکرز مجرمانہ وجوہات، جیسے معلومات چرانے یا ان کے ای میل، بینک یا سوشل میڈیا اکاؤنٹس تک رسائی حاصل کرنے کے لیے، ان کے کمپیوٹر پر کچھ نصب کرنے کی کوشش

کریں گے۔ یا یہ لنک انہیں کسی دوسری ویب سائٹ (بینک کے نقلی ورژن) تک لے جا سکتی ہے جو ان سے ان کی آئی ڈی، پاسورڈ یا بینک کی دیگر تفصیلات مانگتی ہے۔ ایک بار جب وہ یہ معلومات ویب سائٹ کو دیتی ہیں تو ہو سکتا ہے کہ انہوں نے اسکیمرز کو اپنا بینک اکاؤنٹ اور پیسہ حوالے کر دیا ہو۔

آپ کا بینک ای میل، فون یا متنی پیغام کے ذریعہ آپ سے رابطہ نہیں کرے گا اور ذاتی تفصیلات نہیں طلب کرے گا۔ اگر آپ کو کبھی شبہ ہو کہ کیا واقعی آپ کا بینک آپ کو کال کر رہا ہے، اور یہ وشنگ اسکیم نہیں ہے تو کال بند کر دیں اور آن لائن ان کا کسٹمر سروس نمبر تلاش کریں۔ واپس کال کرنے سے پہلے 5 منٹ انتظار کریں یا دوسرا فون استعمال کریں کیوں کہ اسکیمرز فون لائنیں ہائی جیک کر سکتے ہیں۔

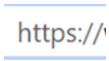
آپ سے بات کرنے کے بعد:

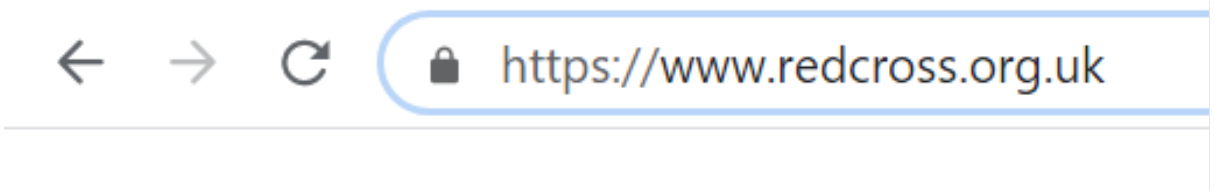
زہرہ آن لائن اپنے بینک کے کسٹمر سروسیز کا ٹیلیفون نمبر تلاش کرتی ہیں۔ بینک تصدیق کرتا ہے کہ یہ ایک نقلی ای میل ہے اور ان کا اکاؤنٹ ٹھیک کام کر رہا ہے۔ وہ انہیں بتاتے ہیں کہ ای میل میں دیا گیا لنک ایک ویب سائٹ کے پاس چلا گیا تھا جو بینک کی ویب سائٹ ہونے کا بہانہ کر رہی تھی۔ کبھی کبھی اس قسم کے دھوکے کے شکار افراد کے لیے اپنی رقم واپس پانا مشکل ہو سکتا ہے، اگر بینک دکھا سکتا ہے کہ وہ محتاط نہیں تھے۔

فشنگ اور اسکیمرز سے متعلق مزید معلومات نیشنل سائبر سیکورٹی سنٹر پر مل سکتی ہے۔
www.ncsc.gov.uk/guidance/phishing

محفوظ اور غیر محفوظ ویب سائٹیں

یہ جانچ کرنے کا اہل ہونا اہم ہے کہ آیا کوئی ایسی ویب سائٹیں جنہیں آپ دیکھتی ہیں وہ محفوظ ہیں۔ کوئی ایسی ویب سائٹ جسے آپ دیکھتی ہیں غیر محفوظ ثابت ہو سکتی ہے، یا آپ کو نقلی ای میلز بھیجنے والے ہیکرز آپ کو کسی ایسی نقلی ویب سائٹ کی طرف بھیج سکتے ہیں جو بہت حقیقی معلوم ہو سکتی ہے۔

براؤزر بار میں یہ پیڈلاک لوگو  یا یہ حروف  تلاش کریں جن کا مطلب ہے کہ کوئی ویب سائٹ محفوظ ہے۔



کبھی کبھی آپ **پیڈلاک** اور **https** دونوں، یا صرف پیڈلاک کی علامت، دیکھیں گی، جس کا انحصار کمپیوٹر یا براؤزر پر ہے۔ ہو سکتا ہے کہ صرف **http** کے ساتھ والی ویب سائٹ محفوظ نہ ہو کیوں کہ **'s'** اشارہ کرتا ہے کہ یہ محفوظ ہے۔

اگر آپ سے کسی اکاؤنٹ میں لاگ-ان کرنے، ادائیگی کی تفصیلات یا دیگر معلومات فراہم کرنے کے لیے کہا جاتا ہے تو دیکھیں کہ کوئی بھی ایسی ویب سائٹ جسے آپ استعمال کر رہی ہیں اس کے براؤزر بار میں پتہ کے آغاز میں "https" موجود ہے۔ صرف اسی وقت لاگ-ان کی تفصیلات داخل کریں جب آپ کو یقین ہو کہ یہ صحیح ویب سائٹ کا پتہ ہے اور یہ کہ یہ محفوظ ہے۔

اپنے بینک کا ویب پیج دیکھنے کے لیے ہمیشہ مکمل ویب پیج پتہ داخل کریں، خاص طور پر اگر آپ آن لائن بینکنگ کے لیے لاگ-ان کر رہی ہیں۔ اپنے بینک کی ویب سائٹ تک پہنچنے کے لیے کبھی کسی سرچ انجن کا استعمال نہ کریں، کیوں کہ یہ قدم ہیکرز کے ذریعہ تحفظ کے ساتھ سمجھوتہ کرنے اور آپ کی تفصیلات چرانے کے لیے استعمال کیا جا سکتا ہے۔

فشنگ اور اسکیم ویب سائٹوں کے خلاف کارروائی کریں

خود کو محفوظ رکھنے کے لیے درج ذیل کار آمد اشارے یاد رکھیں:

- اپنا براؤزر سافٹ ویئر، اینٹی وائرس اور اسپائی ویئر اپ-ٹو-ڈیٹ رکھیں
- ایسی خطرناک ویب سائٹوں سے گریز کریں جو محفوظ نہیں ہیں یا جن پر پیڈلاک نہیں ہے
- کسی ایسے ای میل میں کسی لنک پر کلک نہ کریں جو کسی غیر معلوم یا مشتبہ ذریعہ کی طرف سے ہو

- ای میل یا فون پر کبھی اپنی ذاتی تفصیلات، پاسورڈز یا سیکورٹی کوڈز نہ فراہم کریں

اگر آپ کسی اسکیم کے ذریعہ ہدف بنائی گئی ہیں تو کیا کریں

اس ای میل، کال، پیغام یا ویب سائٹ کی اطلاع دیں۔

اگر آپ کو کوئی ای میل موصول ہوا ہے اور آپ کو اس کے بارے میں معلوم نہیں ہے تو آپ اسے **سسپیشیس ای میل رپورٹنگ سروس (Suspicious Email Reporting Service (SERS))** کو report@phishing.gov.uk پر دے سکتے ہیں۔ وہ آپ کو بتائیں گے کہ آیا یہ فشنگ ای میل ہے یا لگتا ہے۔

اگر آپ کو کوئی مشکوک متنی پیغام موصول ہوتا ہے تو آپ اسے مفت میں 7726 پر بھیج سکتے ہیں۔ یہ آپ کے فون مہیاکنندہ کو اس متن کی تفتیش کرنے اور اگر یہ کوئی اسکیم ہے تو کارروائی کرنے کا موقع فراہم کرتا ہے۔

اپنی تفصیلات شیئر نہ کریں بلکہ اس کی جانچ کریں۔ ای میل میں دئے گئے نمبر پر کبھی کال نہ کریں یا لنکس پر کلک نہ کریں کیوں کہ وہ آپ کی رہنمائی کسی نقلی اکاؤنٹ کی طرف کر سکتے ہیں۔ اس کی بجائے آن لائن ہوں اور وسیع پیمانے پر اشتہارات والا نمبر تلاش کریں اور اس پر کال کریں۔

اس پر سوال کیے بغیر لنکس کو فالو نہ کریں کہ وہ آپ کو کہاں لے جا رہے ہیں۔ یہ جانچ کرنے کے لیے کہ آیا کوئی ویب سائٹ حقیقی ہے، اپنا ویب براؤزر کھولیں اور URL بار میں نام ٹائپ کرتے ہوئے براہ راست جائیں۔

اپنا پاسورڈ یا پن نمبر کبھی شیئر نہ کریں۔ اس سے کوئی مطلب نہیں ہے، اگر آپ سمجھتی ہیں کہ پوچھنے والا شخص آپ کی والدہ یا آپ کا بہترین دوست ہے – اپنا پاسورڈ نہ فراہم کریں۔

اگر دھوکے سے آپ سے اپنے بینک کی تفصیلات فراہم کرا لی گئی ہیں تو فورا اپنے بینک کو بتائیں۔

اگر آپ کے پیسے ضائع ہوگیے ہیں تو اپنے بینک کو بتائیں اور ایک جرم کی حیثیت سے اس کی اطلاع **ایکشن فراڈ (Action Fraud)** (انگلینڈ، ویلز اور ناردرن آئرلینڈ کے لیے) اور یا **پولیس اسکاٹ لینڈ (Police Scotland)** (اسکاٹ لینڈ کے لیے) کو دیں۔ ایسا کرتے ہوئے آپ دوسروں کو شکار بننے سے روکنے میں مدد بھی کریں گی۔

ایکشن فراڈ www.actionfraud.police.uk

آن لائن رشتے

اس سیکشن میں ہم ذاتی رشتوں پر انٹرنیٹ کے اثر کے بارے میں بات کریں گے۔ ہم جو کچھ آن لائن کرتے ہیں وہ براہ راست ہماری نجی زندگی کو متاثر کر سکتے ہیں۔ اس لیے، اس معلومات کے بارے میں بہت محتاط رہنا اہم ہے جو آپ آن لائن دوسروں کے ساتھ شیئر کرتی ہیں۔

ہم سب دیگر لوگوں کے ساتھ مربوط ہونا چاہتے ہیں، اور یہ انٹرنیٹ کی سب سے بڑی خوبی ہے کہ ہم پوری دنیا میں دوستوں، خاندان کے افراد اور مشترک مفادات کے حامل لوگوں کے ساتھ بہ آسانی مواصلات کر سکتے ہیں۔ ساتھ ہی ساتھ، یہ سمجھنا بھی اہم ہے کہ آن لائن روابط کو دھیان سے منظم رکھنے کی ضرورت ہے، بالکل گلی میں کسی شخص سے ملنے کی طرح، اور یہ کہ دوسرے لوگ برے خیال کے ساتھ لوگوں سے رابطے قائم کرنے کے خواہاں ہو سکتے ہیں جو بدسلوکی کا باعث بن سکتا ہے۔

آن لائن بدسلوکی مکمل طور پر اجنبی یا ایسے لوگوں کی طرف سے ہو سکتی ہے جو آپ کے لیے پہلے سے جانے پہچانے ہوں، اور ہم ذیل میں آن لائن باہمی بدسلوکی کی کچھ مثالوں پر نظر ڈالیں گے۔

رومان کا دھوکہ

رومان کا دھوکہ اس وقت ہوتا ہے جب کوئی شخص، اعتماد حاصل کرنے کے لیے باہمی رشتہ استوار کرتے ہوئے، آن لائن ڈیٹنگ ویب سائٹ یا ایپ کا استعمال کرتا ہے اور پھر پیسے یا ذاتی معلومات طلب کرتا ہے۔ وہ رشتہ بنانے کے لیے امکانی طور پر کوئی نقلی پروفائل استعمال کر رہے ہوں گے، اور وہ حقیقی اور دھیان رکھنے والے معلوم ہو سکتے ہیں۔ اکثر و بیشتر یہ بہت سارے ذاتی سوالات پوچھیں گے، لیکن اپنے بارے میں بہت زیادہ نہیں دکھائیں یا بتائیں گے۔ وہ اس وقت تک

انتظار کریں گے جب تک کہ ان کو اعتماد نہ ہو جائے کہ انہوں نے بھروسہ بنا لیا ہے اور وہ مدد، عام طور پر پیسے، مانگنے کے لیے جذباتی وابستگی کا استعمال کرتے ہیں، لیکن یہ بھی کوئی پارسل وصول کرنے یا کوئی پتہ مہیا کرنے کے لیے ہو سکتا ہے۔ وہ اپنی جھوٹی تصاویر یا فوٹو بھی بھیج سکتے ہیں، جو اکثر انٹرنیٹ پر کہیں اور سے لی جاتی ہیں۔

کسی ایسے شخص کو **کبھی نہ** پیسے بھیجیں یا اس سے وصول کریں یا اسے اپنے بینک کی تفصیلات فراہم کریں جس سے آپ آن لائن ملتی ہیں، اس سے کوئی مطلب نہیں کہ آپ ان پر کتنا بھروسہ کرتی یا ان کی کہانی پر یقین رکھتی ہیں۔

دھوکے سے یہ سوچنے کا احساس دلایا جانا واقعی پریشان کن یا سراسیمہ کرنے والا ہو سکتا ہے کہ آپ نے آن لائن ایک خاص رشتہ یا دوستی بنا لی ہے، بلکہ آپ اس کی اطلاع ایکشن فراڈ کو دے سکتی ہیں یا 0300 123 2040 پر کال کر سکتی ہیں۔

کسی امیج کے ذریعہ کی جانچ کرنے کے لیے آپ ایک *ریورس امیج سرچ* کر سکتی ہیں، جو جیسا کہ نام بتاتا ہے، آپ کو ان جیسے دیگر لوگوں کو تلاش کرنے کے لیے انٹرنیٹ امیجیز میں آپ کو سرچ کرنے کا موقع فراہم کرتا ہے۔ آپ ریورس امیج جانچ یہاں کر سکتی ہیں۔

سائبر-بلنگ (دھونس جمانا)

سائبر بلنگ آن لائن یا ٹیکنالوجی کا استعمال کرتے ہوئے دھونس جمانے اور ہراساں کرنے کے لیے ایک عمومی اصطلاح ہے۔ یہ آن لائن بدسلوکی کی ایسی کسی بھی قسم کا احاطہ کرتی ہے جو کسی دوسرے شخص کو نقصان پہنچانے، پریشان کرنے یا ذاتی نقصان پہنچانے کے مقصد سے کی گئی ہو۔ اکثر دھونس جمانے والے افراد سوشل میڈیا کی نیٹ ورکنگ سائٹس جیسے فیس بک (Facebook) یا ٹویٹر (Twitter)، میسیجنگ یا متعامل فورمز کا استعمال کرتے ہیں۔ سائبر بلنگ خاص طور پر پریشان کن ہو سکتی ہے کیوں کہ یہ، صرف کسی مخصوص حالت جیسے اسکول یا مقام کار کی بجائے، انٹرنیٹ اور موبائل فونز کے واسطہ سے کسی بھی وقت لوگوں تک پہنچ سکتی ہے۔

اگر کسی نے آپ کے بارے میں انٹرنیٹ یا سوشل میڈیا پر جھوٹی یا پرعناد چیزیں پوسٹ کی ہیں تو اسے ہراسانی تصور کیا جا سکتا ہے جو ایک جرم ہے۔ اسی طرح، اگر آپ کو ایسی کالیں موصول ہوتی ہیں جو آپ کو دھمکی دیتی یا ڈراتی ہیں تو ہو سکتا ہے کہ یہ چیزیں کرنے والا شخص ایک قابل تعزیر جرم کا ارتکاب کر رہا ہو۔

دھونس جمانے کا عمل، بچوں اور بالغان دونوں سمیت، کسی کو بھی متاثر کر سکتا ہے لیکن اگر آپ بچوں کے پیرنٹ یا نگہدار ہیں تو اس سے آگاہ رہنا خاص طور پر اہم ہے۔ اگر آپ یا آپ کے بچہ یا کسی اور کے ساتھ دھونس جمایا جاتا ہے، جس میں آن لائن بلنگ بھی شامل ہے، تو آپ صلاح کے لیے نیشنل بلنگ ہیلپ لائن کو 0300 323 0169 پر کال کر سکتی ہیں۔

گرومنگ

گرومنگ اس وقت ہوتی ہے جب کوئی کسی شخص کے ساتھ رشتہ کا اعتماد اور ربط بناتا ہے تاکہ وہ ان کا استحصال کر سکیں اور انہیں کنٹرول کر سکیں۔ بچوں اور کمسن شخص کی آن لائن گرومنگ خاص طور پر تشویش کی بات ہوتی ہے، جس میں کوئی کمسن فرد (آن لائن یا شخصی) جنسی بدسلوکی، منشیات کے لین دین کے مقاصد کے لیے یا استحصال کے دیگر مقاصد کے لیے تیار کیا جا سکتا ہے۔

گرومنگ مختصر یا طویل مدت تک پیش آسکتی ہے اور گرومرز بچہ کے خاندان کے ساتھ بھی رشتہ بنا سکتے ہیں تاکہ وہ انہیں قابل اعتماد، معتبر اور معاون ہونے کا احساس دلا سکیں۔ اپنی نسل، جنس، عمر اور بچہ کے ساتھ اپنے رشتہ سے قطع نظر کوئی بھی شخص گرومر ہو سکتا ہے۔

گرومنگ آن لائن پیش آسکتی ہے جس میں گرومر خود کو بچہ کا ہم عمر ظاہر کر سکتا ہے اور دوسرے لوگوں کی ایسی تصاویر یا ویڈیوز بھیج سکتا ہے جو اس کی تائید کرتی ہوں۔ وہ کھیل کھیل سکتے ہیں، صلاح دے سکتے ہیں، سمجھ بوجھ کا مظاہرہ کر سکتے ہیں اور کمسن شخص کے لیے تحائف خرید سکتے ہیں تاکہ ایک قابل اعتماد دوست کی حیثیت سے اپنی پوزیشن مضبوط کر سکیں، یا بچہ کو خاندان یا دوستوں سے علیحدہ کرنے کی کوشش کر سکتے ہیں، کسی عمل یا عدم عمل کے ضمن میں بچہ کو عار دلانے کے لیے بلیک میلنگ کا استعمال کر سکتے ہیں، یا بچہ کو کنٹرول کرنے کے لیے "راز" ("secrets") کا آئیڈیا متعارف کرا سکتے ہیں۔

اس بارے میں دیگر ذرائع کے ساتھ ساتھ گرومنگ سے متعلق مزید معلومات NSPCC کی ویب سائٹ سے دستیاب ہے کہ بدسلوکی اور آن لائن دھمکیوں کے بارے میں بچوں سے کس طرح بات کریں۔ www.nspcc.org.uk

اگر آپ کو شبہ ہے کہ کوئی بچہ خطرے میں ہے تو پولیس کو بتانے میں تردد نہ کریں۔ آپ آن لائن بدسلوکی کی اطلاع دینے سے متعلق صلاح اور تعاون کے لیے NSPCC سے بھی رابطہ کر سکتی ہیں۔

سیکسٹنگ اور انتقامی فحاشی

سیکسٹنگ اس وقت ہوتی ہے جب کسی دوسرے شخص کو جنسی پیغام، تصویر یا ویڈیو بھیجی جاتی ہے۔ کوئی شخص خود اپنی یا کسی دوسرے شخص کی تصویر بھیج سکتا ہے۔ **سیکسٹ** آن لائن کسی دوست، پارٹنر یا کسی اور کو بھیجا جا سکتا ہے، اور اس میں جزوی یا کلی عریانیت، جنسی لحاظ سے واضح انداز میں تصویر کھنچانا یا جنسی اعمال کے بارے میں بات کرنا شامل ہو سکتا ہے۔

جب کہ دو رضامندی ظاہر کرنے والے فریقوں کے مابین جنسی پیغام بھیجا جا سکتا ہے، لیکن تصاویر زیر بحث فرد کی رضامندی کے بغیر انٹرنیٹ پر بہت جلدی شیئر کی جا سکتی ہیں۔ اگر کسی شخص نے آن لائن کوئی تصویر یا ویڈیو شیئر کی ہوں تو وہ کسی کو بھی بھیجی جا سکتی ہیں۔

انتقامی فحاشی اس وقت ہوتی ہے جب کوئی شخص کسی شخص کی **نجی جنسی** تصویر یا فلم، زیر بحث فرد کی رضامندی کے بغیر اور **ان کے لیے پریشانی کا باعث بننے کے ارادے** سے کسی دوسرے شخص یا لوگوں کو دکھاتا یا شائع کرتا ہے۔

کسی شخص کو اس کی نجی معلومات اور تصاویر کا انکشاف کرنے کی دھمکی دینا بھی بلیک میل اور ایک قابل تعزیر جرم ہے۔ انتقامی فحاشی سے متعلق مزید معلومات یہاں دستیاب ہے

ریوینج پورن ہیلپ لائن – 0845 6000 459

www.revengepornhelpline.org.uk/

کسی کے لیے کسی دوسرے شخص پر عریاں تصاویر بھیجنے کے لیے دباؤ ڈالنا کبھی بھی ٹھیک نہیں ہے۔

یہ یاد رکھنا اہم ہے کہ، اسنیپ چیٹ (Snapchat) جیسی خدمات کا استعمال کرتے ہوئے بھی، بھیجی جانے والی تصاویر کی اسکرین شاٹ لی جا سکتی ہے اور محفوظ کی جا سکتی ہیں۔ اگر آپ نے کوئی عریاں یا جنسی تصویر بھیجی ہے اور آپ فکرمند ہیں کہ کیا ہو سکتا ہے تو آپ ان کار آمد اشاروں کے واسطہ سے کارروائی کر سکتی ہیں:

- پیغام حذف کرنے کے لیے کہیں۔
- دھمکیوں کا جواب نہ دیں۔
- کسی سے بات کریں اور مدد طلب کریں۔ آپ ریوینج پورن ہیلپ لائن سے رابطہ کر سکتی ہیں۔
- **جو کچھ ہوا ہے اس کی رپورٹ کریں۔** آپ بدسلوکی پر مبنی مواد کی اس ویب سائٹ پر رپورٹ کر سکتی ہیں جس پر تصاویر شائع ہوئی ہیں۔ زیادہ تر سوشل میڈیا پلیٹ فارمز مواد کی رپورٹ کرنے کے لیے ایک ٹول رکھتے ہیں۔ آپ کو اس قسم کی ہراسانی کی رپورٹ پولیس میں بھی کرنی چاہیے: اگر یہ کوئی ایمرجنسی نہیں ہے تو 101 پر کال کریں۔

اس چیز سے آگاہ ہونا اہم ہے کہ سیکسول آفینسیز ایکٹ 2003 کے تحت **18 سال سے کم عمر کے کسی شخص** کی عریاں تصویر شیئر کرنا بچہ کے ساتھ بدسلوکی ہے اور ایک قابل تعزیر جرم ہے۔ 18 سال سے کم عمر کے کسی شخص کا 'سیکسٹ' کسی اور کے پاس بھیجنے کے نتیجہ میں پولیس تفتیش ہو سکتی ہے۔

اگر آپ بچوں کی تصاویر شیئر کیے جانے کے بارے میں فکرمند ہیں یا آپ کو آن لائن بچوں کے تحفظ کے بارے میں دیگر تشویشات لاحق ہیں تو آپ ان کی رپورٹ چائلڈ اکسپولائٹیشن اینڈ آن لائن پروٹیکشن کے سیفٹی سنٹر میں کر سکتی ہیں۔
www.ceop.police.uk

سائبر-اسٹاکنگ اور نظر رکھنا

اسٹاکنگ (تعاقب) کسی دوسرے کی طرف سے رویہ کا ایسا انداز ہے جو آپ کو خوف دلاتا ہے کہ آپ کے خلاف تشدد کا استعمال کیا جائے گا یا جو آپ کے لیے خطرے یا پریشانی کا باعث بنتا ہے اور آپ کی معمول کی روز مرہ سرگرمیوں پر سنگین اثر ڈالتا ہے۔ جب یہ آن لائن ہوتی ہے تو اسے سائبر اسٹاکنگ کہا جاتا ہے۔ یہ آپ کے بارے میں معلومات جمع کرنا، خود کو آپ کے طور پر پیش کرنا، ان چاہے یا دھمکی آمیز پیغامات بھیجنا، آپ پر نظر رکھنا یا آپ کے آن لائن اکاؤنٹ تک

رسائی حاصل کرنا اور آپ کے بارے میں غلط معلومات پھیلانا ہو سکتا ہے۔ اسٹاکر آپ کا کوئی جانا پہچانا یا اجنبی بھی ہو سکتا ہے۔ سائبر اسٹاکنگ اپنے شکار پر سنگین اثر ڈال سکتی ہے اور یہ ایک قابل تعزیر جرم ہے۔

نیشنل اسٹاکنگ ہیلپ لائن – 0808 802 0300

www.stalkinghelpline.org/faq/about-the-law/

اگر آپ کو تشویش ہے کہ کسی بدسلوکی کرنے والے فرد کے ذریعہ آپ کو اسٹاک کیا جا رہا یا آپ پر نظر رکھی جا رہی ہے تو:

- اسٹاکر کے ساتھ شامل ہونے سے گریز کریں، جو اکثر آپ سے بات کرنا اور آپ کے ساتھ رشتہ بنانا چاہتا ہے۔ ان سے ملنے پر کبھی اتفاق نہ کریں اور ان کا سامنا نہ کریں۔
- اسے سنجیدگی سے لیں اور اس سرگرمی کی اطلاع پولیس میں دیں۔ آپ براہ راست پولیس سے بات کرنے کے لیے 101 پر کال کر سکتی ہیں لیکن اگر آپ سمجھتی ہیں کہ فوری خطرہ پایا جاتا ہے تو 999 ڈائل کریں۔
- اپنی پرائیویسی سیٹنگس کی جانچ کریں، یقینی بنائیں کہ آپ کے بارے میں آن لائن کم سے کم معلومات دستیاب ہو، اور اپنے آلہ پر لوکیشن ٹیگنگ کو بند کر دیں۔
- اپنے آس پاس کے لوگوں کو متنبہ کر دیں۔ انہیں یہ جانچ کرنے کی ضرورت پڑ سکتی ہے کہ وہ آپ کے بارے میں کیا شیئر کر رہے ہیں اور ان کی پرائیویسی سیٹنگس کی بھی جانچ کرنے کی ضرورت پڑ سکتی ہے۔
- جو کچھ ہوتا ہے اس کا ایک ریکارڈ رکھیں – آپ کالوں، پیغامات یا سوشل میڈیا کی پوسٹس کی اسکرین شاٹ بھی لے سکتی ہیں، جس کا مطلب یہ ہے کہ آپ کے پاس ثبوت کی ایک نقل ہے، خواہ مرتکب جرم اپنے پیغامات حذف کر دے اور بعد میں پوسٹ کرے۔

گھریلو بدسلوکی، ہراسانی اور نظر رکھنا

ایک بدسلوکی کرنے والا فرد کسی شکار پر نظر رکھنے، حقیقت حال معلوم کرنے اور اسے کنٹرول کرنے کے لیے امکانی طور پر ایسے آلہ کے فیچرز کا غلط استعمال کر سکتا ہے جس پر انٹرنیٹ چالو ہو۔ اس میں دوسرے لوگوں کے ساتھ آپ کی مواصلات پر نظر رکھنا، آپ کے آلہ کے واسطہ سے آپ کے محل وقوع کا پتہ لگانا، یا آپ کے مالی خرچ کی جانچ کرنا بھی شامل ہو سکتا ہے۔ جب ان رویوں کا ارتکاب کسی پارٹنر، سابق پارٹنر، خاندان کے فرد یا نگہدار کے ذریعہ کیا جاتا ہے تو یوکے کے قانون کے تحت یہ سب گھریلو بدسلوکی کی شکلیں تصور کی جاتی ہیں۔

اگر آپ فکرمند ہیں کہ ہو سکتا ہے کوئی آپ کے موبائل فون یا کسی دیگر آلہ پر نظر رکھ رہا ہو تو نیشنل ڈومیسٹک ابیوز ہیلپ لائن اسے زیادہ محفوظ رکھنے کی خاطر سیٹنگس تبدیل کرنے میں آپ کی مدد کرنے کے لیے ایک واک-تھرو ٹول رکھتی ہے۔

نیشنل ڈومیسٹک ابیوز ہیلپ لائن (24 گھنٹے) 0808 220 0247

www.nationaldomesticviolencehelpline.org.uk

کیا آپ درج ذیل بیانات سے اتفاق کرتی ہیں؟

آن لائن دھمکیاں کوئی اہمیت نہیں رکھتی ہیں کیوں کہ یہ 'حقیقی' دنیا نہیں ہے۔

نہیں۔ آن لائن بدسلوکی سنگین چیز ہے، یہ لوگوں کی زندگیوں پر سنگین اثر ڈالتی ہے اور حکام کے ذریعہ ہمیشہ اسے سنجیدگی سے لیا جانا چاہیے۔ اسٹاکنگ، نظر رکھنا، اور ہراسانی یہ سب زیادہ خطرے والے رویے ہیں جو آپ کی غلطی نہیں ہے۔ آپ کو ان کی رپورٹ کرنے، صلاح لینے اور ان پر توجہ دینے کے لیے تعاون کیے جانے کا حق حاصل ہے۔

ہراسانی کے جرم کا مطلب ہے حقیقی زندگی میں تشدد کی دھمکی دیا جانا۔

قانون بیان کرتا ہے کہ ہراسانی اس وقت ہوتی ہے جب کوئی شخص ایسے انداز میں برتاؤ کرتا ہے جس کا مقصد آپ کے لیے پریشانی یا خطرے کا سبب بننا ہو اور یہ رویہ ایک سے زیادہ بار پیش آتا ہو۔ الگ الگ مواقع یا معاملات میں رویہ کی قسمیں مختلف ہو سکتی ہیں۔ مثال کے طور پر، آپ کو پریشان کرنے کے مقصد سے ایک پیغام ہراسانی نہیں ہے۔ دو پیغامات ہراسانی ہو سکتے ہیں، یا کسی فون کال کے بعد دھمکی آمیز ای میل ہراسانی ہو سکتا ہے۔ ایسی دیگر سرگرمیاں جو ہراسانی شمار کی جاتی ہیں اس صورت میں ہو سکتی ہیں جب آپ کا تعاقب کیا جاتا ہو، آپ کے گھر یا کام پر نظر رکھی جاتی ہو، آپ کی املاک کو نقصان پہنچایا جاتا ہو، یا جب پرعناد اور جھوٹے طریقہ سے آپ کی رپورٹ پولیس میں کرائی جاتی ہو جب کہ آپ نے کچھ غلط نہیں کیا ہے۔

زہرہ کی ایک کزن ہیں جن سے وہ بہت قریب ہیں۔ ان کی کزن حال ہی میں پریشان اور چڑچڑی نظر آتی ہوئی الگ طریقہ سے عمل کر رہی تھیں اور اس وقت پریشان حال انداز میں اپنی فون کال چیک کر رہی تھیں جب وہ ساتھ ہوتی تھیں۔ بالآخر، زہرہ کی کزن انہیں بتاتی ہیں کہ وہ اچھی طرح سو بھی نہیں سکی ہیں اور وہ اپنے سابق شوہر کی طرف سے دی جانے والی دھمکیوں سے بہت پریشان ہیں، جن سے وہ الگ ہو رہی ہیں۔ وہ انہیں برابر میسیج بھیجتا ہے اور یہ کہنے کے لیے ای میل بھیجتا ہے کہ وہ بہت نالائق عورت اور والدہ ہیں، اور وہ ان کے دونوں خاندانوں کے لیے شرم کا باعث بنی ہیں، اور یہ کہ ان کا واپس آنا اور ان کے ساتھ رہنا ضروری ہے۔ زہرہ کی کزن اسے دوبارہ یاد کرتے ہوئے انتہائی پریشان ہیں۔

وہ وضاحت کرتی ہیں کہ ان کے سابق شوہر کے پاس ان کی عریاں تصویر ہے، جو انہوں نے ایک ساتھ اس وقت لی تھیں جب ان کا رشتہ زیادہ بہتر تھا۔ اس نے عریاں تصویر ان کے خاندان والوں کو بھیجنے کی دھمکی دی ہے، اگر وہ اس کے پاس واپس نہیں جاتی ہیں۔

کیا زہرہ کی کزن جرم کی شکار ہے؟

ہاں۔ زہرہ کی کزن **ہراسانی اور جبری کنٹرول** کی شکار ہیں۔ زہرہ کی کزن کو یہ دھمکیاں ان پر کنٹرول رکھنے کے لیے دی گئی ہیں۔ قانون بیان کرتا ہے کہ یہ جرم اس وقت ہوتا ہے جب کوئی شخص ایسا رویہ اختیار کرتا ہے جس کا مقصد آپ کے لیے پریشانی یا خطرے کا باعث بننا ہو۔ ضروری ہے کہ یہ رویہ ایک سے زیادہ بار پیش آتا ہو۔

چوں کہ یہ رویہ ان کے سابق شوہر کے ذریعہ اختیار کیا جاتا ہے، اس لیے یہ ہراسانی **جبری کنٹرول** (ایک قسم کی **گھریلو بدسلوکی**) کی ایک شکل ہے۔ یہ ایک قابل تعزیر جرم ہے۔ انہیں اس کی اطلاع پولیس میں دینی چاہیے۔

یہ پریشانی یا ندامت کا باعث بننے کے مقصد سے انتقامی فحاشی، رضامندی کے بغیر ان کی نجی جنسی تصاویر شیئر کرنے، کی دھمکی بھی ہے۔ دھمکی بذات خود کسی جرم کے ہم معنی نہیں ہے، تاہم اگر زہرہ کا سابق شوہر اسے آن لائن، ای میل یا سوشل میڈیا بشمول وہاٹس ایپ یا پیغام رسانی کی دیگرخدمات کے ذریعہ، شیئر کرتا ہے تو یہ ایک جرم بن جائے گا۔

زہرہ کا شوہر خاندان کی عزت و وقار اور ان کی علیحدگی کا خاندان کے لیے "ندامت" کا باعث ہونے کے بارے میں بھی بات کرتا ہے۔ نام نہاد 'عزت و وقار' پر مبنی تشدد بدسلوکی کی ایک شکل ہے اور زہرہ کسی ایسی تنظیم سے تعاون حاصل کر سکتی ہیں جو عزت و وقار پر مبنی بدسلوکی اور دھمکیوں کے شکار افراد کے ساتھ کام کرنے میں خصوصی مہارت رکھتی ہو۔ **کرما نروان (Karma Nirvana)** پیر تا جمعہ ایک ٹیلیفون ہیلپ لائن چلاتی ہے 0800 5999 247
www.karmanirvana.org.uk

خلاصہ

- پوسٹ کرنے سے پہلے سوچیں۔ اس بارے میں غور کرنے سے پہلے چیزیں اپلوڈ یا شیئر نہ کریں کہ اگر یہ غلط ہاتھوں میں پڑ جائے تو آپ کیسا محسوس کریں گی۔ جب آپ کوئی چیز پوسٹ کر دیتی ہیں تو اس پر آپ کا کنٹرول نہیں رہتا ہے، بالخصوص اگر کوئی اس کی اسکرین شاٹ لے لیتا ہے۔
- اپنی شناخت کی حفاظت کریں اور ہر چیز سوشل میڈیا پر نہ شیئر کریں۔ سوشل میڈیا دوستوں اور خاندان کے افراد کو رابطہ میں رہنے کا موقع دینے کے لیے شاندار چیز ہے لیکن اس بارے میں سوچیں کہ آیا آپ دنیا کو اس سے زیادہ بتانا چاہیں گی جتنا آپ چاہتی تھیں۔

- اس پر دھیان سے غور کریں کہ جو کچھ آپ آن لائن شیئر کر رہی ہیں اسے کون دیکھ سکتا ہے، جانچ کریں کہ آپ کی پرائیویسی سیٹنگس اعلی درجہ پر مرتب کی گئی ہیں اور سوچیں کہ آپ کس سے بات کر رہی ہیں۔
- اسکیمز کی علامات اور اس بارے میں آگاہ رہیں کہ اسکیم ای میلز اور ویب سائٹیں کس طرح تلاش کریں
- بہت زیادہ نجی معلومات آن لائن کبھی نہ ظاہر کریں جیسے آپ کا پتہ، فون نمبر، پورا نام، تاریخ پیدائش۔
- اپنی لاگ-ان کی تفصیلات اور پاسورڈز کبھی نہ فراہم کریں۔
- نامعلوم ای میلز، فائلیں یا منسلکات کبھی نہ کھولیں اور فشنگ اور اسکیمز سے آگاہ رہیں