BritishRedCross

ریفیوجی خواتین

ڈیجیٹل تفویض اختیار اور کنیکٹ پروجیکٹ

سیشن 3 – ڈیجیٹل حفاظت

Home Office

The power of kindness

خوش آمدید!

آج ہم:

- ضروری ڈیجیٹل حفاظت کے اقدامات اور انٹرنیٹ تحفظ سے متعلق تجاویز پر گفتگو کریں گے

- عام آن لائن دھمکی کی قسمیں کو شناخت کرنے کے طریقے پر گفتگو کریں گے

- آن لائن حفاظت کے اقدامات کو سوشل میڈیا اور حقیقی زندگی کے بین شخصی رشتوں سے مربوط کرنے کے طریقے پر گفتگو کریں گے

بنیادی اصول

- خفیہ جگہ
- محفوظ جگہ
- فونز خاموشی پر
- مؤدب بنیں
- غیر فیصلہ کن
- ایک بار میں ایک سے بات کریں
- اگر بات نہیں کر رہے ہیں تو Zoom کو میوٹ پر رکھیں
- **اگر آپ کسی بات کا اعادہ کروانا چاہتے ہیں تو ضرور کہیں!**

- معلوم نہیں ہونا ٹھیک ہے

ڈیجیٹل حفاظت

مضبوط پاس ورڈ رکھنا

See Metropolitan Police (2017) #threerandomwords
https://www.youtube.com/watch?v=3aY_EPgi0VU

- اپنے پاس ورڈز کو مشکل بنائیں، تاکہ دوسرے لوگ آسانی سے اس کا اندازہ نہ لگا سکیں
- پاس ورڈز باقاعدگی سے تبدیل کریں
- ہر اکاؤنٹ کے لیے ایک ہی پاس ورڈ مت استعمال کریں
- سکیورٹی سوالات سیٹ کریں مبادا آپ اپنا پاس ورڈ بھول جائیں
- مضبوط پاس ورڈ بنانے کے لیے، ایک تجویز یہ ہے کہ تین اتفاقی الفاظ منتخب کریں، انہیں ایک ساتھ ملائیں اور ان میں اعداد، بڑے حروف اور علامات شامل کریں جیسے Cat!PotatoS0fa7

The power of kindness

وائرسوں سے اپنی ڈیوائسز کا تحفظ کرنا

- کمپیوٹرز، فونز اور دیگر ڈیوائسز میں وائرس آ سکتے ہیں جن کی وجہ سے کافی نقصان ہو سکتا ہے۔
- اینٹی وائرس سافٹ ویئر ایک کمپیوٹر پروگرام ہے جو وائرسوں کو روکنے، ان کا پتہ لگانے اور انہیں ہٹانے کے لیے استعمال ہوتا ہے۔
- آپ کا لیپ ٹاپ 12 ماہ کے Windows Defender اینٹی وائرس کے ساتھ سیٹ اپ کیا ہوا ہے۔ اس کے بعد، آپ کے لیپ ٹاپ میں رواں سافٹ ویئر تحفظ موجود ہونے کو یقینی بنانا آپ کی ذمہ داری ہے۔
- اینٹی وائرس سافٹ ویئر کو باقاعدگی سے اپ ڈیٹ کرنا ہوتا ہے۔

آن لائن دھمکی کی عمومی قسمیں

ای میل کے گھوٹالے	فشنگ	مضر سافٹ ویئر – 'میلویئر'
- **ای میل یا متنی پیغام، اکثر جن کا ہدف آپ کو ایک لنک پر کلک کرنے پر مائل کرنا ہوتا ہے۔** - کلک کر دینے پر، آپ کو ایک غیر محفوظ ویب سائٹ پر بھیجا جا سکتا ہے جو آپ کے کمپیوٹر پر وائرس ڈاؤن لوڈ کر سکتا ہے، یا آپ کے پاس ورڈز اور ذاتی معلومات کو چرا سکتا ہے۔ - اس میں ایسی زبان استعمال ہو سکتی ہے جو 'کارروائی کریں' کا دباؤ پیدا کرتی ہے جیسے لنک کھولیں، تفصیلات دیں یا اٹیچمینٹ پر کلک کریں۔	- ایسے پیغامات جو **آپ کو حساس معلومات** جیسے ذاتی ڈیٹا **فراہم کرنے کے جال میں پھانسنے** کی کوشش کرتے ہیں؛ - پیغامات کافی حقیقی اور مائل کن نظر آ سکتے ہیں اور اکثر کسی بینک یا دیگر بھروسہ مند مآخذ سے آئے ہوئے معلوم پڑتے ہیں - ہو سکتا ہے آپ پاس ورڈ دوبارہ درج کرنے، تاریخ پیدائش کی تصدیق کرنے یا کریڈٹ کارڈ نمبر کی تصدیق کرنے کے خواہاں ہوں؛ - آپ کی ذاتی تفصیلات تک رسائی حاصل ہو جانے پر، مجرمین اسے فراڈ والے جرائم جیسے شناخت کی چوری اور بینک فراڈ انجام دینے کے لیے استعمال کرتے ہیں۔	- ایسا سافٹ ویئر جو کسی کے ذریعے ڈیوائسز کو نقصان پہنچانے کے لیے بنایا گیا ہو۔ - کبھی کبھار آپ کی ڈیوائس پر محفوظ کردہ معلومات یا ڈیٹا اکٹھا کرتا ہے، اور اسے آگے بڑھا دیتا ہے۔ - یہ **رینسم ویئر، وائرس، وورم، ٹروجن، ہارس، اسپائی ویئر، ایڈ ویئر، اسکیئر ویئر** اور **کرائم ویئر** کے بطور بھی معروف ہے۔

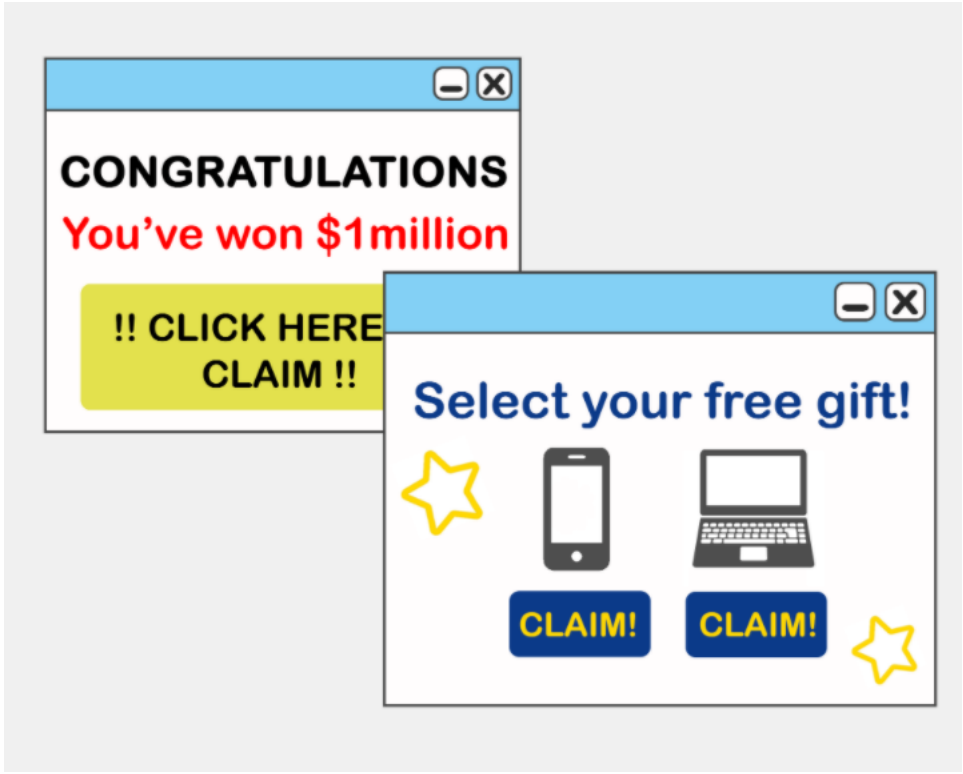
فشنگ اور گھوٹالے والی ای میلز کو پہچاننا

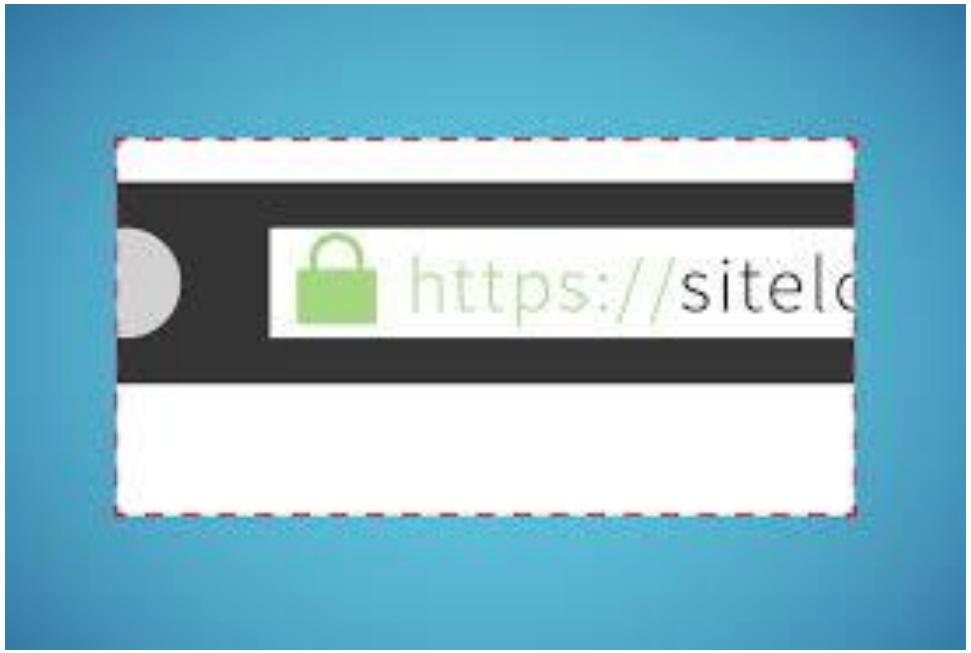
- کیا آپ مرسل کو جانتے ہیں؟ کیا وہ عمومی تہنیت میں آپ کو مخاطب کر رہے ہیں؟
- کیا اس میں املا کی غلطیاں ہیں یا یہ ناقص انداز میں تحریر کی گئی ہے؟
- کیا یہ آپ سے کوئی کام کروانا چاہتی ہے یا کیا اس میں فوری طلب ہونے کا شعور ہے یا کیا یہ آپ کو دھمکی دے رہی ہے؟
- کیا یہ درست ہونے کی حد تک اچھی معلوم پڑتی ہے؟
- وہ ای میل پتہ کھولیں جس سے پیغام بھیجا گیا ہے۔ کیا اس میں درست ڈومین نام ہے؟
- کیا یہ غیر متوقع یا ایسی کمپنی کی جانب سے ہے جس کے ساتھ آپ کا کاروبار نہیں ہے؟
- کیا یہ آپ کو دوسری ویب سائٹ پر لے جاتی ہے؟

The power of kindness

محفوظ ویب سائٹس

ویب سائٹس پر 'پاپ اپس' اکثر معتبر نہیں ہوتے ہیں۔

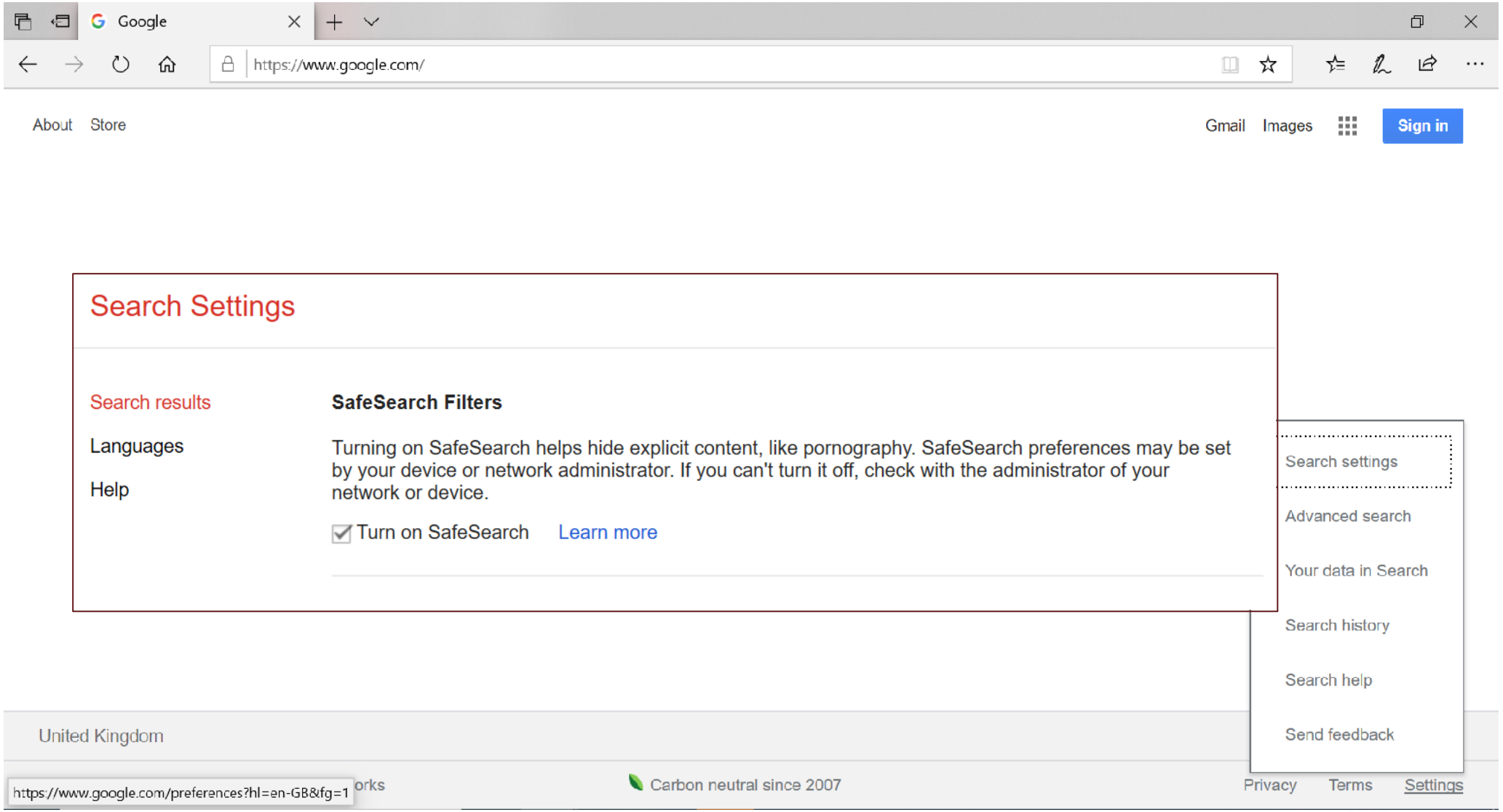




پیڈلاک کی علامت اور/یا https کی علامت چیک کر کے دیکھیں کہ آیا ویب سائٹ محفوظ ہے

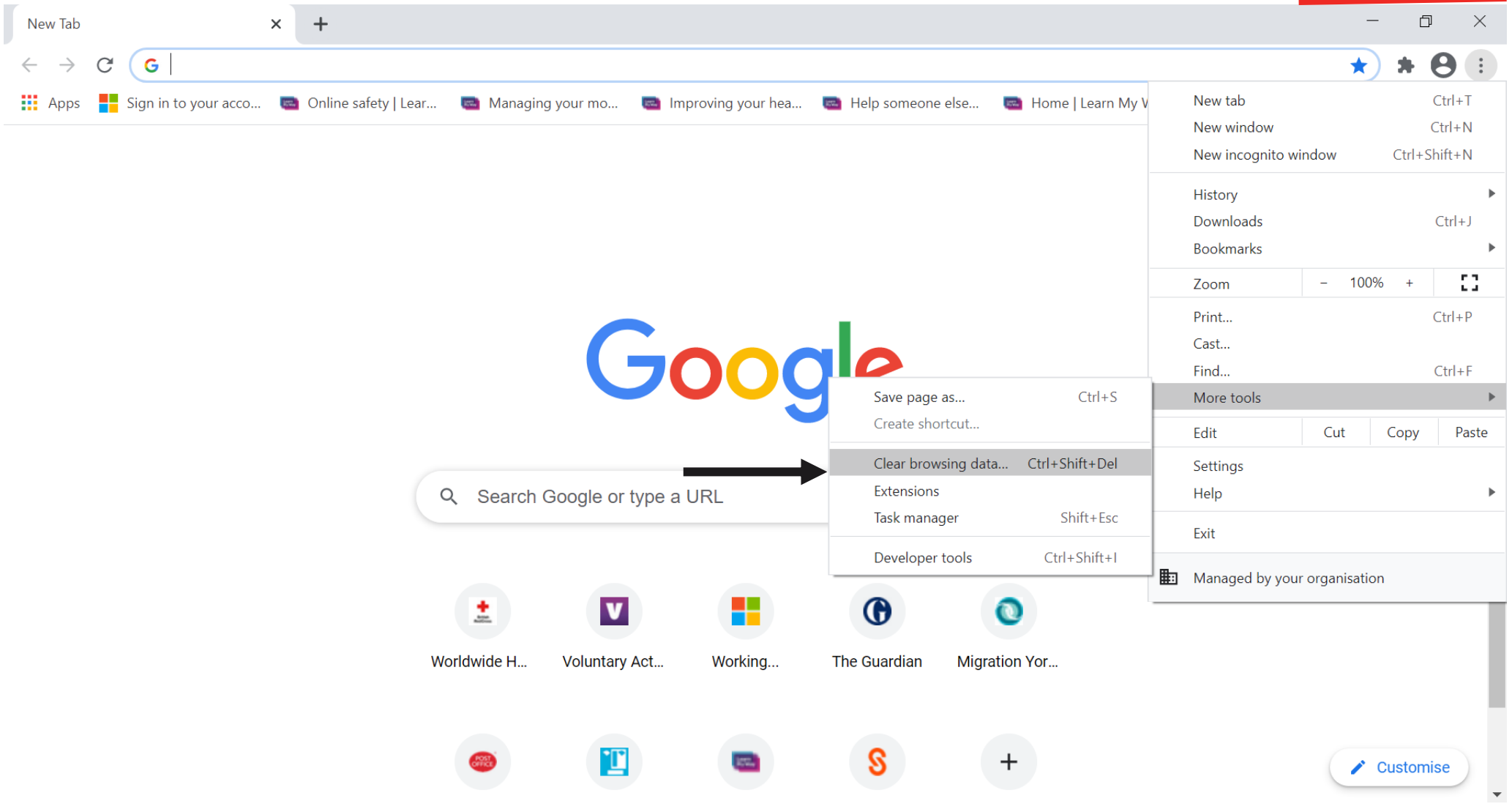
The power of kindness

محفوظ تلاش



The power of kindness

تلاش کی سرگزشت کو صاف کرنا



The power of kindness

لوگوں سے آن لائن جڑنا

- سوشل میڈیا کے لیے رازداری کی ترتیبات
- سرچ انجنوں پر سوشل میڈیا کے مشمولات

The power of kindness

رومانس کا فراڈ

- اعتماد حاصل کرنے کے لیے ایک بین شخصی رشتہ فروغ دینا اور پھر پیسے یا ذاتی معلومات طلب کرنا۔
- اعتماد کے فروغ اور مدد، عموماً پیسہ طلب کرنے کے لیے جذباتی وابستگی کا استعمال ہوتا ہے، لیکن یہ پارسل موصول کرنے یا کوئی پتہ مہیا کرنے کے لیے بھی ہو سکتا ہے۔

سائبر ایذا رسانی

- ایذا رسانی جو آن لائن یا ٹیکنالوجی کا استعمال کر کے ہوتی ہے۔
- ایذا رساں افراد اکثر سوشل میڈیا نیٹ ورکنگ سائٹس جیسے فیس بک یا ٹویٹر، پیغام رسانی یا باہم متعامل فورمز کا استعمال کرتے ہیں۔
- بالغان اور بچے دونوں کو متاثر کر سکتا ہے۔

بہلانا

- کسی فرد کے ساتھ رشتے کا اعتماد اور میل جول پیدا کرنا تاکہ وہ، اکثر جنسی بدسلوکی کے مقاصد سے ان کا استحصال اور انہیں کنٹرول کر سکیں۔
- آن لائن بچوں اور نوعمر افراد کو بہلانا بچے کے ساتھ بدسلوکی کی ایک شکل ہے۔

سیکسٹنگ اور انتقامی پارن

- دوسرے فرد کے نجی، جنسی مواد، یا تو تصاویر یا ویڈیوز، ان کی منظوری کے بغیر اور سراسیمگی یا تناؤ پیدا کرنے کے مقصد سے شیئر کرنا۔
- نابالغوں کی تصاویر شیئر کرنا بچے کے ساتھ بدسلوکی ہے۔

سائبر تعاقب اور مانیٹرنگ

- تعاقب کرنا دوسرے فرد کی جانب سے اس رویے کا ایک طرز ہے جس سے خوف یا تناؤ پیدا ہوتا ہے۔ جب یہ آن لائن ہو تو اسے سائبر تعاقب کے بطور جانا جاتا ہے۔
- سائبر تعاقب کے شکار فرد پر اس کے سنگین اثرات مرتب ہو سکتے ہیں اور یہ ایک تعزیری جرم ہے

گھریلو بدسلوکی

- نفسیاتی، جسمانی، جذباتی یا مالی بدسلوکی جو پارٹنر، سابق پارٹنر، فیملی ممبر یا نگراں کی جانب سے انجام پاتی ہے۔
- بدسلوک فرد شکار کو دیکھنے، اس پر نگاہ رکھنے اور اسے کنٹرول کرنے کے لیے انٹرنیٹ کا یا انٹرنیٹ سے فعال شدہ ڈیوائسز کا امکانی طور پر غلط استعمال کرتا ہے۔

رشتے آن لائن

The power of kindness

زہرہ کی ایک کزن ہے جس سے وہ کافی قریب ہے۔ اس کی کزن مختلف انداز کی حرکت کرتی رہی تھی جو حال ہی میں پریشان، چڑچڑی معلوم پڑتی تھی، اور جب وہ ساتھ ہوتے تو وہ ہر وقت سراسیمگی کے انداز میں اپنا فون چیک کرتی تھی۔ آخر کار، زہرہ کی کزن نے اسے بتایا کہ وہ اچھی طرح سے سو نہیں پا رہی تھی اور اپنے سابق شوہر کی طرف سے دی جانے والی دھمکیوں سے وہ کافی تناؤ زدہ تھی، جس سے وہ علیحدہ ہو رہی ہے۔ وہ باقاعدگی سے اسے پیغام بھیجتا تھا اور ای میل بھیج کر کہتا تھا کہ وہ ایک خوفناک بیوی اور ماں ہے، اور اس نے دونوں فیملیز کو شرمسار کر دیا ہے، اور یہ کہ اسے چاہیے کہ واپس ہو جائے اور اس کے ساتھ رہے۔ زہرہ کی کزن اسے یاد کرتے ہوئے انتہائی افسردہ ہے۔

وہ مزید بتاتی ہے کہ اس کے سابق شوہر کے پاس اس کی ایک ننگی تصویر ہے، جو انہوں نے اس سے پہلے اپنے رشتے میں ساتھ مل کر لی تھی۔ اگر وہ واپس نہیں ہوتی ہے تو اس نے وہ ننگی تصویر اس کی فیملی کو بھیجنے کی دھمکی دی ہے۔

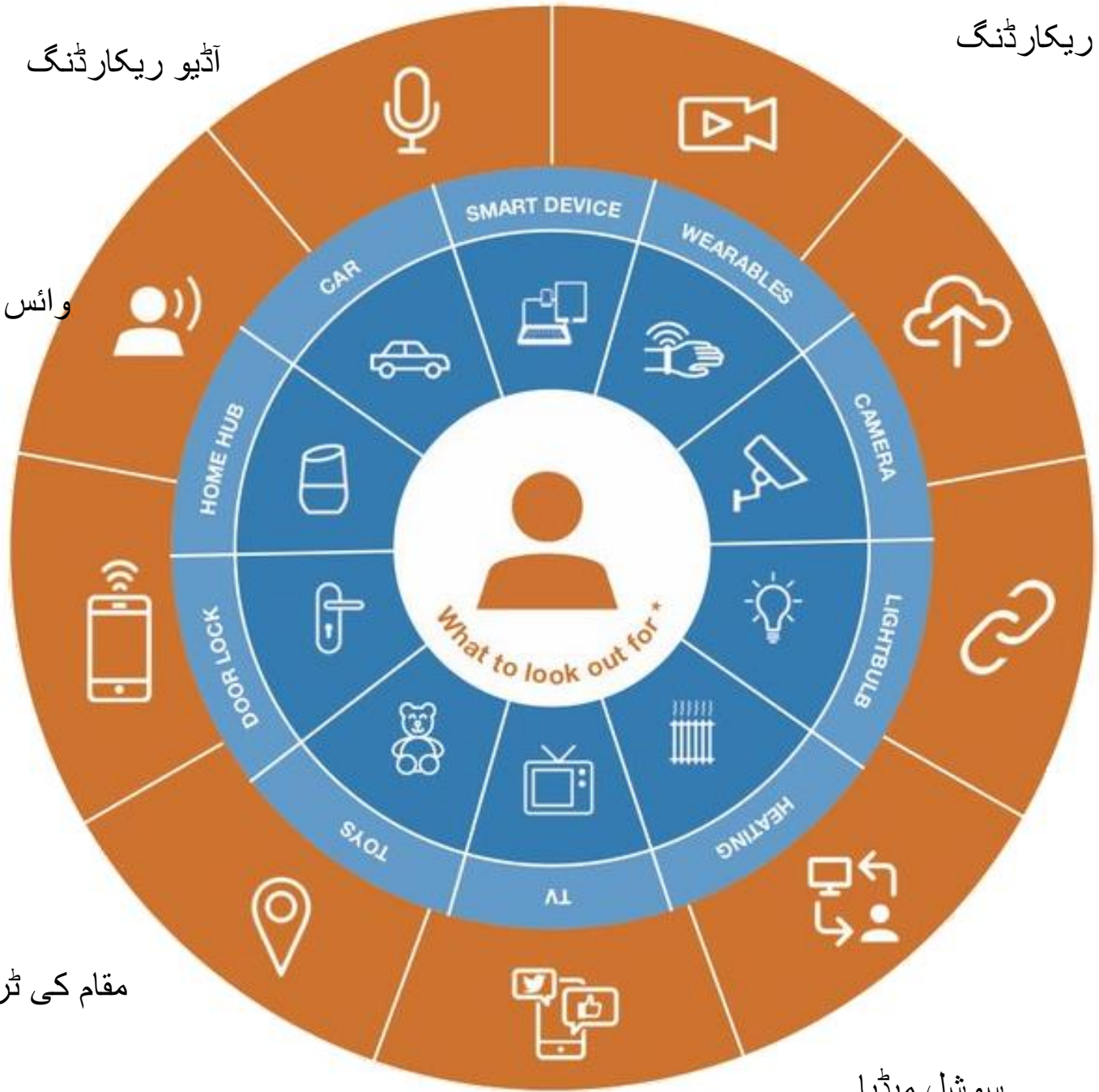
ڈیجیٹل حفاظت کو بہتر بنانا

ڈیجیٹل ڈیوائس کیا ہیں؟

آپ کون سا سوشل میڈیا استعمال کرتے ہیں؟

آپ کا مشورہ کیا ہوگا؟

The power of kindness



آڈیو ریکارڈنگ

ویڈیو ریکارڈنگ

وائس کنٹرول

ڈیٹا اکٹھا کرنا

ریموٹ کنٹرول

شیئر کردہ اکاؤنٹس

مقام کی ٹریکنگ

مشین لرننگ

سوشل میڈیا

The power of kindness

ڈیجیٹل حفاظت کو بہتر بنانا

تشخیص کریں	تشخیص کریں کہ آپ کے بارے میں کون سی معلومات آن لائن جیسے فیس بک یا ٹویٹر پر موجود ہیں
تبدیل کریں	کلیدی آن لائن اکاؤنٹ کیلئے اپنی ای میل اور پاس ورڈز تبدیل کریں
حذف کریں	موجود آن لائن اکاؤنٹس کو حذف کریں خاص طور پر اگر وہ کافی مقدار میں معلومات یا تصاویر پر مشتمل ہوں۔
جائزہ لیں	رازداری اور سکیورٹی کی تمام ترتیبات کا جائزہ لیں
احتراز کریں	عوامی فورمز سے احتراز کریں
محدود کریں	آپ جو کچھ شیئر کرتے ہیں اسے محدود کریں
حذف کریں	آپ Chrome, Firefox, Internet Explorer اور Safari پر اپنی تلاش کی سرگزشت کو حذف کر سکتے ہیں۔
سیٹ اپ کریں	اپنے کمپیوٹر یا موبائل ڈیوائسز کے لیے پاس ورڈ یا PIN سیٹ اپ کر کے یقینی بنائیں کہ صرف آپ ہی اس تک رسائی حاصل کر سکتے ہیں۔
ای میل	ای میل: اپنی ای میل کے لیے ایسا پاس ورڈ منتخب کرنا ضروری ہے جس کا دوسرے فرد کے لیے اندازہ لگانے کا امکان نہ ہو۔

خلاصہ

آج ہم نے:

- ڈیجیٹل حفاظت کے لیے بنیادی تجاویز پر گفتگو کی
- عمومی آن لائن دھمکی کی کچھ مثالوں اور انہیں پہچاننے کے طریقوں پر گفتگو کی
- آپ کی آن لائن رازداری اور ڈیجیٹل حفاظت کو چیک کرنے اور بہتر بنانے کی تجاویز پر گفتگو کی۔

سب سے اہم طور پر، ڈیجیٹل حفاظت آن لائن واقفیت کے بارے میں ہے۔

The power of kindness

کلیدی الفاظ

ڈیوائس – الیکٹرانک ایکوپمنٹ جو انٹرنیٹ سے مربوط ہو سکتی ہے

ڈیجیٹل واقفیت – انٹرنیٹ اور انٹرنیٹ سے جڑی ڈیوائس استعمال کرنے میں فوائد اور خطرات کی جانکاری کو فروغ دینا

ڈیجیٹل حفاظت – انٹرنیٹ استعمال کرتے وقت خود کو، دوسروں کو اور اپنی ذاتی معلومات کو محفوظ رکھنے کے طرز عمل اور عادات

آن لائن بدسلوکی – دوسرے فرد کا ظالمانہ اور نقصان پہنچانے والا برتاؤ جو انٹرنیٹ کی معرفت انجام پاتا ہے

آن لائن دھمکی – وہ خطرہ یا مسئلہ جو انٹرنیٹ کی معرفت ناپسندیدہ واقعے یا عمل کا سبب بنتا ہے

پاس ورڈ - حروف کا ایک خفیہ سلسلہ جو کمپیوٹر سسٹم یا سروس تک رسائی کی اجازت دیتا ہے

رازداری کی ترتیبات – کنٹرولز جنہیں سوشل میڈیا پر قابل رسائی معلومات کو کھولنے یا محدود کرنے کے لیے استعمال کیا جا سکتا ہے۔

سوشل میڈیا – وہ ویب سائٹس اور کمپیوٹر پروگرامز جنہیں کمپیوٹر یا موبائل فون کا استعمال کر کے، انٹرنیٹ پر مواصلت کرنے یا معلومات شیئر کرنے کے لیے لوگ استعمال کرتے ہیں۔