

پاس ورڈ

شرکاء مضبوط پاس ورڈز کا استعمال اور اہتمام کر کے اپنی آن لائن معلومات کو مزید محفوظ رکھنے کا طریقہ جانیں گے۔ شرکاء مضبوط پاس ورڈ بنانے کے اصولوں کے بارے میں اور پاس ورڈ کا اشتراک کرنے پر پیش آ سکنے والے ممکنہ مسائل کے بارے میں جانیں گے۔ وہ اپنے پاس ورڈز کو محفوظ رکھنے اور اپنے اکاؤنٹس تک غیر مجاز رسائی کو روکنے کے لیے اقدام کرنے کے طریقے بھی جانیں گے۔

مواد

پاس ورڈ کے متعلق جاننے کا ہینڈ آؤٹ

پاس ورڈ سے متعلق بنیادی باتیں

حصہ 1

اپنے طلباء کو بتائیں

ہم اکثر ویب سائٹس، ایپس اور سروسز کے لیے اپنے زیر استعمال پاس ورڈز کے بارے میں زیادہ نہیں سوچتے ہیں۔ تاہم، جتنے اچھے آپ کے پاس ورڈز ہوتے ہیں وہی تعین کرتے ہیں کہ آپ کی معلومات کتنی محفوظ ہوگی۔

جماعت میں تعامل

مندرجہ ذیل سوالات استعمال کر کے گفتگو میں شرکاء کو مصروف کریں۔ براہ کرم شرکاء کو یاد دلائیں کہ اس یا دوسرے کسی بھی عمل کے دوران ان کے اصل پاس ورڈز کا اشتراک نہ کرنا اہم ہے۔

اپنے طلباء سے پوچھیں

آپ کے پاس کتنے پاس ورڈز ہیں؟

کیا آپ کے پاس اپنی ہر ای میل اور سوشل میڈیا اکاؤنٹ کے لیے الگ الگ پاس ورڈز ہیں۔

کیا وہ کافی الگ ہیں یا وہ واحد پاس ورڈ کی قسم ہیں؟

اگر آپ کے پاس ایک سے زیادہ پاس ورڈ ہیں تو آپ یہ کیسے یاد رکھتے ہیں کہ کون سا پاس ورڈ کس اکاؤنٹ کا ہے؟

اپنے طلباء سے پوچھیں

آپ اہم پاس ورڈ کتنی بار بھول چکے ہیں؟

جب آپ اپنا پاس ورڈ بھول گئے تو آپ نے کیا کیا؟

آپ اپنے پاس ورڈز یاد رکھنے کو آسان کیسے بناتے ہیں؟

کیا کوئی ایسا پاس ورڈ ہے جسے آپ روزانہ استعمال کرتے ہیں؟

کیا ہوگا اگر — آپ کی معلومات کے بغیر — کسی کو معلوم ہو جائے کہ آپ کا پاس ورڈ کیا ہے؟

کیا یہ اس پر منحصر ہوگا کہ یہ کون ہے؟

اگر کسی شخص نے آپ کے اکاؤنٹ میں داخل ہونے کے لیے آپ کا پاس ورڈ استعمال کر لیا ہے تو وہ آپ کے بارے میں کس طرح کی معلومات حاصل کر سکتا ہے؟

حصہ 2

جماعت میں تعامل

شرکاء کو جوڑیوں میں منظم کریں۔

اپنے طلباء کو بتائیں

اپنے پارٹنر کے ساتھ، بات کریں کہ اگر کسی ایسے شخص کو آپ کے پسندیدہ سوشل میڈیا پلیٹ فارم کا پاس ورڈ پتہ چل جائے جو نقصان پہنچانا چاہتا ہے تو کیا ہوسکتا ہے۔

جماعت میں تعامل

بات کرنے کے لیے شرکاء کو 5 منٹ کا وقت دیں۔ اور گروپس سے اشتراک کرنے کو کہیں۔

اپنے طلباء کو بتائیں

اب اپنے پارٹنر سے اس بارے میں بات کریں کہ اگر کسی پیکر کو آپ کے والدین / نگہداشت فراہم کنندہ کے آن لائن بینکنگ اکاؤنٹ کے پاس ورڈ کا پتہ چل جائے تو کیا ہوگا۔

جماعت میں تعامل

بات کرنے کے لیے شرکاء کو 5 منٹ کا وقت دیں۔ پھر، گروپس سے اس چیز کے اشتراک کا مطالبہ کریں جس پر انہوں نے بات کی ہے۔

حصہ 3

اپنے طلباء کو بتائیں

آپ کو یہ جان کر حیرانی ہوسکتی ہے کہ پیکر نجی پاس ورڈ کیسے جان سکتے ہیں۔ کچھ طریقے موجود ہیں؛ ایک طریقہ سوشل انجینئرنگ ہے — یا کسی کو اپنے پاس ورڈ کا اشتراک کرنے کے لیے جال میں پھنسانا۔ پیکر ایسی ای میل بھیج کر یہ کر سکتا ہے جو ہو بہو ایسا لگتا ہے کہ یہ کسی ایسے پلیٹ فارم یا ویب سائٹ سے درست طریقے سے آئی ہے جس پر کسی کا اکاؤنٹ موجود ہے۔ ای میل اس شخص سے لنک پر کلک کرنے اور اپنے صارف نام اور پاس ورڈ کے ساتھ لاگ ان کرنے کا مطالبہ کر سکتی ہے؛ جب وہ شخص لاگ ان کرتا ہے تو یہ معلومات پیکر کے لیے دستیاب ہو جاتی ہے۔

بعض اوقات پیکرز عام جملوں جیسے "password123"، "test"، یا آپ کے پہلے اور آخری نام کا استعمال کر کے پاس ورڈز کا اندازہ لگانے کی کوشش کرتے ہیں۔

دوسرا طریقہ جس سے پیکرز نجی پاس ورڈ جانتے ہیں اسے "بروٹ فورس" حملہ بولتے ہیں۔ بروٹ فورس حملہ اس وقت ہوتا ہے جب پیکر بار بار مختلف پاس ورڈز آزما کر آپ کے اکاؤنٹ میں لاگ ان کرنے کی کوشش کرتا ہے۔ چونکہ پیکر ہاتھ سے "بروٹ فورس" حملہ کر سکتا ہے، یہ اکثر کمپیوٹر پروگرام چلا کر کیا جاتا ہے جو تیزی سے اور خود بخود پاس ورڈز کے ہر ممکن جوڑے کو بنانے کی کوشش کرتا ہے جسے یہ سوچ سکتا ہے۔ مثال کے طور پر، ممکنہ پاس ورڈز کی فہرست یا مختلف حروف اور اعداد کے مجموعہ پر مشتمل پاس ورڈز کا سیٹ، جب تک انہیں صحیح پاس کوڈ نہ ملے۔

واقعہ، کچھ "بروٹ فورس" حملے زیادہ نئے ہوتے ہیں۔ اگر آپ کا پاس ورڈ ممکنہ پاس ورڈز کی فہرست میں ہے جیسے "fido123" یا "password"، اس کے بعد کچھ پروگرام کم امکان یا بے ترتیب امکانات والوں سے پہلے ان اختیارات کو آزما کر تیزی سے اس کا اندازہ لگا سکتے ہیں۔ اگر ہیکر آپ کے بارے میں جانتا ہے تو حملہ اور بھی زیادہ بہتر ہو سکتا ہے۔ مثال کے طور پر، اگر ہیکر جانتا ہے کہ آپ کے پالتو جانور کا نام ٹوبی ہے تو وہ 'ٹوبی' کے آخر میں الگ الگ نمبروں (جیسے 'Toby629' یا 'Toby3020') سے آزما کر دیکھتا ہے۔

ڈیزائن کے اصول

حصہ 1

اپنے طلباء سے پوچھیں

کون جانتا ہے کہ "مضبوط" یا "مضبوط ترین" پاس ورڈ سے کیا مراد ہے؟ یہ ایک اچھا خیال کیوں ہے؟

اپنے طلباء کو بتائیں

ایک مضبوط پاس ورڈ سے آپ کی معلومات کی حفاظت میں مدد ملتی ہے۔ ایک مضبوط پاس ورڈ رکھنے کے باوجود اس بات کی ضمانت نہیں ہوتی ہے کہ آپ کا اکاؤنٹ ہیک نہیں ہو گا، لیکن کمزور پاس ورڈ کسی کے لیے آپ کی معلومات تک رسائی حاصل کرنے کو آسان بناتا ہے۔

پاس ورڈ کی مشق

اپنے طلباء سے پوچھیں

کمزور پاس ورڈ کی کچھ مثالیں کیا ہیں؟

1. مثالوں میں شامل ہیں: پاس ورڈ، 12345، پیلو!، تاریخ پیدائش، عرفی نام۔

آپ انہیں کمزور کیوں خیال کرتے ہیں؟

1. کسی دوسرے شخص کی طرف سے اور / یا ایسے کمپیوٹر کے ذریعہ جس پر "بروٹ فورس" چل رہا ہو، ان کا آسانی سے اندازہ لگایا جا سکتا ہے۔

ایسے کچھ طریقے کیا ہیں جن کے ذریعہ آپ پاس ورڈ مضبوط بنا سکتے ہیں؟

1. نمبرز، بڑے اور چھوٹے حروف، علامات شامل کرنا، پاس ورڈ کو طویل کرنا، اور عام جملے اور الفاظ کے استعمال سے بچنا۔

جماعت میں تعامل

شرکاء کے ذریعہ ان کے ان پٹ فراہم کیے جانے کے بعد، بورڈ پر ان ہدایات کو لکھیں:

کم از کم ایک نمبر شامل کریں۔

کم از کم ایک سمبل شامل کریں۔

کم از کم ایک بڑا حرف اور ایک چھوٹا حرف شامل کریں۔

پاس ورڈ کم از کم 7 حروف والا ہونا چاہیے۔

پاس ورڈز ایسے ہوں کہ انہیں یاد رکھنا آسان ہے (الا یہ کہ آپ پاس ورڈ منیجر کا استعمال کر رہے ہوں)۔

پاس ورڈ منیجر ایسی ویب سائٹ / ایپ ہے جو صارفین کو اپنے پاس ورڈز محفوظ رکھنے اور انہیں منظم کرنے میں مدد کرتی ہے۔

پاس ورڈز کوئی عام مفرد لفظ یا ذاتی معلومات (پیدائش کی تاریخ، والدین کا نام، وغیرہ) نہیں ہونا چاہیے۔

مختلف ویب سائٹس کے پاس ورڈز مشترکہ نہیں ہونے چاہیے۔

اپنے طلباء کو بتائیں

مضبوط پاس ورڈز بنانے کے دو طریقے ہیں۔ پہلا طریقہ یہ ہے کہ بورڈ پر موجود اس طرح کی "پاس ورڈ ہدایت" کی پیروی کی جائے۔ اس طرح کی ہدایت کا استعمال آپ کی حوصلہ افزائی کرتا ہے کہ آپ متنی / عددی پاس ورڈ میں ایسے عناصر شامل کریں جن کا اندازہ لگانا مشکل ہو جس کی وجہ سے پاس ورڈ بذات خود مشکل ہو جاتا ہے۔ اس طریقہ کا منفی پہلو یہ ہے کہ یہ پاس ورڈز کے یاد رکھنے کو مشکل بنا دیتا ہے۔

مضبوط پاس ورڈز

اپنے طلباء کو بتائیں

مضبوط پاس ورڈز بنانے کا دوسرا طریقہ پاس ورڈ کی لمبائی سے مربوط ہے۔ چونکہ پاس ورڈ کی طاقت پاس ورڈ کی لمبائی سے متعلق ہے، لہذا چار یا اس سے زیادہ غیر متعلقہ الفاظ کا استعمال کرنے سے انسان اور "بروٹ فورس" کے لیے پاس ورڈز کا اندازہ لگانا مشکل بن جاتا ہے۔ اس طریقہ میں اضافی فائدہ ہے جو کہ ہدایت کردہ طریقہ کے مقابلہ میں زیادہ آسانی سے یاد ہونے کی صورت میں ہوتا ہے۔

آخر میں، کوئی علامات اور نمبرز سمیت چار یا اس سے زیادہ غیر متعلقہ الفاظ کی اسٹرنگ استعمال کر کے ان دو طریقوں کے مجموعہ کا استعمال کر سکتا ہے۔

ان مختلف طریقوں کا مقصد یہی ہے: ایسے پاس ورڈز بنانا جو منفرد ہوں اور دیگر لوگوں کے لیے ان کا اندازہ لگانا مشکل ہو۔

اپنے طلباء کو بتائیں

شرکاء کو جوڑوں میں منظم کریں

جوڑوں میں، بورڈ پر اپنی سابقہ تحریر کردہ ہدایات کا استعمال کرتے ہوئے ایک مضبوط پاس ورڈ بنانے کی کوشش کریں۔ یاد رکھیں کہ ایک پاس ورڈ جس کا بغیر ترتیب کے اندازہ لگانا کمپیوٹر کے لیے مشکل ہوتا ہے وہ اب بھی انسان یا ایسے کمپیوٹر کے لیے جس کے پاس عام لمبے پاس ورڈز کی فہرست ہو، آسان ہو سکتا ہے۔ آپ کے پاس ورڈ والا کاغذ کا ٹکڑا سرگرمی کے اختتام پر جمع نہیں کرایا جائے گا۔ آپ کی اس بات کے لیے حوصلہ افزائی کی جاتی ہے کہ آپ فی الواقع اپنے کسی اکاؤنٹ کے لیے اس پاس ورڈ کا استعمال نہ کریں، چونکہ گروپ میں موجود لوگ اسے جان جائیں گے۔

ایسا کرنے کے شرکاء کو 5 منٹ کا وقت دیں۔ اس کے بعد کمرے کے ارد گرد جائیں اور شرکاء سے پوچھیں کہ ان کے خیال میں ان کے مضبوط ترین پاس ورڈ کے نمونے کیا ہیں۔ شرکاء سے پوچھیں آیا وہ اپنے تخلیق کردہ پاس ورڈز براہ راست دیکھے بغیر یاد کر سکتے ہیں۔

اگرچہ کچھ ویب سائٹس کو آپ کے پاس ورڈ کی ضرورت ہوتی ہے تاکہ وہ ان شرائط میں سے چند (یا تمام) کو پورا کر سکیں، دیگر میں اس طرح کی پابندیاں نہیں ہوتیں۔ آپ بے ترتیب عام الفاظ کی ایک اسٹرنگ کا استعمال کر کے بھی پاس ورڈز بنا سکتے ہیں۔

جماعت میں تعامل

اسی جوٹی میں، شرکاء کو نئے پاس ورڈز بنانے دیں جو الفاظ کی سیدھی ترتیب میں ہوں۔ پاس ورڈ کو مضبوط اور آسانی سے یاد رہنے والا بنانے کیلئے ان سے کہیں کہ اس میں کم از کم چار الفاظ ہونے چاہیے۔ ایسا کرنے کے شرکاء کو 5 منٹ کا وقت دیں۔ اس کے بعد کمرے کے ارد گرد جائیں اور شرکاء سے پوچھیں کہ ان کے پاس ورڈ کے نمونے کیا ہیں۔ دوبارہ، شرکاء کو یاد دلائیں کہ سرگرمی کے بعد پیپر کی شیٹ جمع نہیں کی جائے گی، نہ ہی ان کے کسی اکاؤنٹ کیلئے پاس ورڈ کا استعمال کیا جائے گا۔

اپنے طلباء کو بتائیں

کچھ ویب سائٹس آپ کی شناخت کی توثیق کے لیے ایک سسٹم کا استعمال کرتی ہیں جنہیں متعدد عناصر (یا دو عناصر) والی توثیق کہا جاتا ہے۔ یہ ویب سائٹس ون ٹائم کوڈ بھیجنے کے لیے اکثر متنی پیغامات، ایپ یا ای میل کا استعمال کرتی ہیں جس کا آپ کے پاس ورڈ کے ساتھ درج کیا جانا ضروری ہوتا ہے۔

یہ طریقہ سیکورٹی کی ایک اضافی پرت بڑھا کر آپ کے اکاؤنٹس کو زیادہ محفوظ بنا سکتا ہے جس کا توڑنا مشکل ہے۔ مثال کے طور پر، آپ کے اکاؤنٹ میں لاگ ان کرنے کے لیے، کسی شخص کے پاس آپ کے پاس ورڈ کا ہونا اور اس اکاؤنٹ سے منسلک ایپ، آلہ، یا ای میل ایڈریس تک رسائی حاصل ہونا ضروری ہے۔

پاس ورڈ کو محفوظ رکھنا

حصہ اول

اپنے طلباء کو بتائیں

اگرچہ آپ کوئی ایسا پاس ورڈ بناتے ہیں جو کمپیوٹر یا کسی شخص کے لئے کریک کرنا واقعی مشکل ہے، اس کے علاوہ دوسرے طریقے موجود ہیں جن سے پاس ورڈ کمزور ہو سکتا ہے۔

اپنے طلباء سے پوچھیں

وہ دوسرے طریقے کیا ہیں جن سے پاس ورڈ کمزور ہو سکتا ہے؟

1. کچھ مثالیں جن میں یہ شامل ہیں: متعدد اکاؤنٹ کے لئے ایک پاس ورڈ کا دوبارہ استعمال، کوئی ایسا پاس ورڈ استعمال کرنا جو ذاتی معلومات پر مشتمل ہو، ایک ہی پاس ورڈ کا کئی سالوں تک استعمال، اپنا پاس ورڈ بھول جانا۔

کتنی بار آپ کو لگتا ہے کہ آپ کو اپنا پاس ورڈ تبدیل کرنا چاہئے؟

اپنے طلباء کو بتائیں

یہاں تک کہ اچھے پاس ورڈ بھی نقب لگائے یا چوری کئے جا سکتے ہیں، لیکن ایسی چیزیں ہیں جو آپ اپنی حفاظت کے لئے کرسکتے ہیں۔ اگر وہاں ایک ویب سائٹ پر ڈیٹا کی خلاف ورزی ہے جہاں آپ کا اکاؤنٹ ہے، تو اس بات کو یقینی بنائیں کہ آپ اس ویب سائٹ پر ساتھ ہی ساتھ دوسری ویب سائٹ پر جہاں آپ یکساں پاس ورڈ استعمال کرتے ہیں اپنا پاس ورڈ تبدیل کریں گے۔

بہت سے طویل اور پیچیدہ پاس ورڈ کو یاد رکھنا مشکل ہو سکتا ہے۔

اپنے طلباء سے پوچھیں

کیا آپ کو لگتا ہے کہ یہ ایک اچھا خیال ہے کہ ایک کاغذ کے ٹکڑے، یا آپ کے کمپیوٹر پر دستاویزی فائل میں اپنے پاس ورڈ لکھیں؟ کیوں یا کیوں نہیں؟

جماعت میں تعامل

امکانات کا تذکرہ جیسے کوئی وہ کاغذ کا ٹکڑا تلاش کر سکتا ہے یا آپ کے کمپیوٹر پر فائل پر غور کر سکتا ہے۔ وضاحت کریں کہ ایک نقطہ نظر پاس ورڈ مینیجر کا استعمال کرنا ہے، ایک ایسا ایپلی کیشن جس سے صارفین کو ان کے پاس ورڈ کو محفوظ اور منظم کرنے میں مدد ملتی ہے۔

حصہ دوم

اپنے طلباء کو بتائیں

ہر دن، ہم مختلف ویب سائٹس پر بہت مختلف اکاؤنٹس استعمال کرتے ہیں۔ ہر وقت ہر ویب سائٹ پر لاگ ان اور سائن آؤٹ کرنا پیچیدہ ہو سکتا ہے۔

اپنے طلباء سے پوچھیں

کیا آپ نے کبھی کسی ویب سائٹ کے لئے پاس ورڈ کو محفوظ کرنے کے لئے اپنے براؤزر میں "پاس ورڈ کو محفوظ کریں" خصوصیت کا استعمال کیا ہے؟ کیوں یا کیوں نہیں؟

کیا آپ سمجھتے ہیں کہ ویب سائٹ کیسے یاد رکھتی ہے کہ آپ کون ہیں؟

1. وضاحت کے لئے پوچھیں۔ پھر وضاحت کریں کہ ویب سائٹس یاد رکھ سکتی ہیں کہ آپ کسی کوئی کو محفوظ کر کے لاگ ان ہوئے ہیں۔ کوکیز آپ کے کمپیوٹر پر محفوظ کی گئی وہ چھوٹی فائلیں ہیں جو مستقبل میں دوبارہ لاگ ان کرے بغیر ملاحظات کے لئے ویب سائٹ کو یہ جاننے میں مدد کرتی ہیں کہ آپ اور آپ کا کمپیوٹر کون ہیں۔ تاہم، کوکیز کا استعمال ایک ویب سائٹ سے دوسری ویب سائٹ تک آپ کے جانے کو ٹریک کرنے کے لئے بھی کیا جا سکتا ہے۔ یہ ایک ایسا طریقہ ہے جس سے اشتہارات آپ کو ہدف بنا سکتے ہیں۔

کیا آپ کے اپنے کمپیوٹر پر کسی پاس ورڈ کو محفوظ کرنا ٹھیک ہے؟

اپنے طلباء سے پوچھیں

کیا آپ کے کمپیوٹر کا لاگ ان پاس ورڈ ہے؟

کیا ہوتا ہے جب آپ دوسروں کے ساتھ کمپیوٹر کا اشتراک کرتے ہیں؟

1. اس صورت میں، اگرچہ پاس ورڈ فیلڈ میں آپ کا پاس ورڈ سیاہ نقطے یا ستارے سے پوشیدہ ہو سکتا ہے، آپ کے کمپیوٹر کا استعمال کرتے ہوئے دوسرے افراد کو ممکنہ طور پر یہ پتہ چل سکتا ہے کہ آپ کا پاس ورڈ کیا ہے۔ صرف اس لیے کہ آپ اس بات کو نہیں دیکھ سکتے کہ اسکرین پر پاس ورڈ کیا ہے اس کا مطلب یہ نہیں ہے کہ یہ کہیں بھی ذخیرہ نہیں ہوتا ہے۔

اپنے طلباء سے پوچھیں

کیا ایسے کوئی اوقات ہوتے ہیں جب پاس ورڈ کا اشتراک کرنا ٹھیک ہوتا ہے؟ کب؟ کیوں؟

1. کچھ مثالیں شاید ہو سکتی ہیں کہ والدین ان کے پاس ورڈ چاہ سکتے ہیں یا ان کا کسی سروس جیسے Netflix پر کوئی مشترکہ/ خاندانی اکاؤنٹ ہو۔

کیا آپ اپنے پاس ورڈ کو کسی کے ساتھ اشتراک کرتے ہیں؟ اگر ایسا ہے تو، کس کے ساتھ / کیوں؟

اگر آپ کسی کے قریبی دوست ہیں، اور وہ آپ سے کہیں گے "اگر آپ کو میری پرواہ کرتے ہیں" تو کیا یہ پاس ورڈ کا اشتراک کرنے کے لئے حوصلہ افزائی کے طور پر کام کرتا ہے؟ کیوں یا کیوں نہیں؟

اپنے طلباء کو بتائیں

آپ کسی کی پرواہ کرتے ہیں تو اس کے ساتھ پاس ورڈ کا اشتراک کرنے کا انتخاب کر سکتے ہیں، لیکن ان کی پرواہ کا مطلب یہ ضروری نہیں کہ وہ آپ کے آن لائن اکاؤنٹس تک مکمل رسائی کے مستحق ہیں۔

اس مخصوص شخص کے ساتھ اشتراک کرنے سے پہلے اپنے تعلقات کے بارے میں احتیاط سے سوچیں، بشمول وقت کے ساتھ شاید یہ تعلقات بدل سکتے ہیں۔ مثال کے طور پر، والدین / دیکھ بھال کرنے والوں کے ساتھ اشتراک کرنا آپ کے بہترین دوست کے ساتھ اشتراک کرنے کے مقابلے میں بہت مختلف انتخاب ہے۔

اپنے طلباء سے پوچھیں

اگر آپ پاس ورڈ کا اشتراک کرتے ہیں تو آپ کے ساتھ کیا ہوسکتا ہے؟

1. کوئی آپ کے بینک اکاؤنٹس کو پیک کر سکتا ہے، آپ کے روپ میں آن لائن بھیس بدل سکتا ہے یا آپ کے کچھ راز جان سکتا ہے۔

اگر آپ ایک اکاؤنٹ کے پاس ورڈ کا اشتراک کرتے ہیں، تو کیا آپ اس اکاؤنٹ کو مختلف طریقے سے استعمال کریں گے؟

اپنے طلباء سے پوچھیں

اگر کوئی اور یہ دیکھ سکتا ہے کہ آپ کیا کر رہے ہیں تو کیا کوئی ایسی چیزیں ہیں جو آپ Netflix پر نہیں دیکھیں گے یا کسی ای میل میں نہیں لکھیں گے؟

جماعت میں تعامل

مشترک اکاؤنٹ کا استعمال کرتے وقت شرکاء کو ان کے اپنے رویے پر غور کرنا چاہئے۔ انہیں یہ غور کرنا چاہیے کہ ان کی آن لائن سرگرمی کسی اکاؤنٹ پر دیگر صارفین کے لئے نمایاں ہو رہی ہیں۔

اپنے طلباء سے پوچھیں

اگر آپ کا اکاؤنٹ آپ کی مجازی نمائندگی کرتا ہے، جیسے کوئی سوشل میڈیا پروفائل، تو کیا یہ ٹھیک ہے کہ آپ دوسرے لوگوں کو اپنے اکاؤنٹ کا استعمال کرنے کی اجازت دیتے ہیں؟

جماعت میں تعامل

کسی شخص کا آپ کے ہونے کا دکھاوا کرنے اور آپ کے دوستوں کو پیغام بھیجنے کے امکانات پر تبادلہ خیال کریں۔

اپنے طلباء سے پوچھیں

کیا آپ کسی بھی آلات کو جو آپ استعمال کرتے ہیں، اپنے پاس ورڈز کو ذخیرہ کرنے کی اجازت دیتے ہیں؟ کیوں یا کیوں نہیں؟ کیا اس کا مطلب ہے کہ یہ آپ کے ذاتی فون یا کمپیوٹر پر آپ کے پاس ورڈز کو محفوظ کرنا محفوظ ہے؟ کیا ہوتا ہے اگر آپ کسی دوست کو آپ کے فون یا کمپیوٹر استعمال کرنے دیتے ہیں؟

کیا آپ کسی آلات کا دوسروں کے ساتھ اشتراک کرتے ہیں، جیسے خاندان یا دوستوں کے ساتھ؟ کیا آپ اس آلہ پر ایک اکاؤنٹ کا اشتراک کرتے ہیں، یا کیا ہر فرد کے پاس خود کا اکاؤنٹ ہے؟

کیا آپ نے کبھی "عوامی" آلہ استعمال کیا ہے، جیسے لائبریری میں، اسکول میں، یا کہیں اور؟ کیا آپ اس

آلہ پر وہی چیزیں کرتے ہیں جو آپ کہیں اور کر سکتے ہیں؟

حصہ سوم

جماعت میں تعامل

شرکاء کو جوڑیوں میں منظم کریں۔

اپنے طلباء کو بتائیں

آپ کی جوڑیوں میں بحث کریں کہ کیا آپ نے کبھی اسکول میں، لائبریری میں، یا کسی دوسرے کمپوٹ کی ترتیب میں کمپیوٹر پر لاگ ان کیا ہے اور دیکھا ہے کہ کوئی اور ابھی بھی اپنے سوشل میڈیا یا ای میل اکاؤنٹ میں لاگ ان تھا۔ ان سے پوچھیں کہ کیا وہ اس اکاؤنٹ میں دیکھنا یا کچھ اور کرنا چاہیں گے۔

جماعت میں تعامل

شرکاء کو بحث کرنے کے لئے 5 منٹ دیں پھر ان سے اشتراک کرنے کے لئے کہیں۔ گروپ کو اس طرح کے غیر مجازی استعمال کے بارے میں بحث میں شامل کریں۔

اکاؤنٹ تک غیر مجاز رسائی

حصہ اول

جماعت میں تعامل

براہ کرم نوٹ کریں: اس سرگرمی کے مواد کے کچھ حصہ کو "سرگرمی # 1 کو کور کیا گیا ہے: پاس ورڈ سے متعلق بنیادی باتیں"۔ آپ اس مواد کو دوبارہ دیکھنا چاہیں گے یا نہیں یا اسے نظر انداز کرنا چاہیں گے، اس بارے میں ہم آپ پر فیصلہ چھوڑتے ہیں۔

اپنے طلباء کو بتائیں

ممکن ہے کہ دیگر لوگ آپ کے اکاؤنٹ تک رسائی حاصل کریں، بھلے ہی انہیں آپ کا پاس ورڈ پہلے سے نہ معلوم ہو یا وہ آپ کے پاس ورڈ کے اتفاقی اندازہ کی مدد سے رسائی حاصل کریں۔ اگر کسی شخص کو آپ کے بارے میں کافی ذاتی معلومات حاصل ہے تو کافی حد تک ممکن ہے کہ وہ آپ کے پاس ورڈ کا اندازہ لگا لے یا وہ آپ کی کمپنی کے کسی شخص کو آپ کی معلومات فراہم کرنے کے لیے راضی کر سکتا ہے۔ چونکہ وہ آپ کے اکاؤنٹ تک رسائی حاصل کرنے کے لیے ٹیکنالوجی کا استعمال نہیں کر رہے ہیں، لہذا اس قسم کے حملہ کو سوشل پیکنگ یا سوشل انجینئرنگ کہا جاتا ہے۔

اپنے طلباء سے پوچھیں

اگر آپ کبھی بھی ویب سائٹ کا اپنا پاس ورڈ بھول گئے تھے تو اپنا ہاتھ اٹھائیں۔

جب آپ "میں اپنا پاس ورڈ بھول گیا" پر کلک کرتے ہیں تو کیا ہوتا ہے؟

1. ویب سائٹ عام طور پر سیکیورٹی کے سوالات طلب کرتی ہے یا فون نمبر یا ای میل کا استعمال کر کے آپ سے رابطہ کرنے کی کوشش کرے گی۔

ویب سائٹ کون سے سیکیورٹی سوالات طلب کرتی ہیں؟

1. وضاحت کریں کہ کیسے ان میں کچھ ایسے سوالات ہیں جن کا دوستوں یا جاننے والے جواب دے سکتے ہیں یا ان کا اندازہ لگا سکتے ہیں۔ اس کے پالتو جانور کا نام، وہ کہاں پیدا ہوا تھا، اس کی والدہ کا پہلا نام، اس کے پسندیدہ استاد کا نام، اس کے قریب ترین دوست کا نام، اس کے پسندیدہ اسپورٹس ٹیم کا نام جیسے چیزیں۔

اور کس کو آپ کی اس قسم کی معلومات پتا ہو سکتے ہیں؟

جب آپ اپنا پاس ورڈ بھول جاتے ہیں تو ویب سائٹ کس طریقے سے آپ سے رابطہ کرتی ہے؟

اور کس کو آپ کے رابطہ کے شخص تک رسائی حاصل ہو سکتے ہیں؟

اپنے طلباء سے پوچھیں

کیسے کوئی اجنبی شخص سیکیورٹی کے سوالات سے متعلق آپ کے جوابات سے وابستہ معلومات تک

رسائی حاصل کر سکتا ہے؟

1. سوشل میڈیا پوسٹس، عوامی معلومات کی آن لائن تلاشیں، متعدد بار اندازہ لگانا، آپ کے دوستوں سے رابطہ کرنا وغیرہ۔

ذاتی معلومات والی سوشل میڈیا پوسٹس کی کچھ مثالیں کیا ہیں؟

1. مثال کے طور پر، آپ کی بلی کا Instagram، جس میں اس کا نام کیپشن میں لکھا ہوا ہو، تصویر جس میں مقام ٹیک کیا گیا ہو یا عوامی سالگرہ کی پوسٹس۔

آپ کی کے بارے میں مزید جاننے اور اس کے پاس ورڈ کو پیک کرنے کے بارے میں مزید جاننے کے لیے ہیں؟ کرتے کیسے استعمال کا Google

1. اگر سرچ انجن آپ کو کسی شخص کے اسکول کے آن لائن نیوز پیپر میں اس کی نویں کلاس کی تصویر دکھانا ہے تو آپ اس کے نویں کلاس کے استاد کا نام پتا کر سکتے ہیں۔

حصہ دوم

اپنے طلباء کو بتائیں

ایسی معلومات پوسٹ کرنا بہت غیر محفوظ ہو سکتا ہے، جس میں آپ کے سیکیورٹی کے سوالات کے جوابات شامل ہوتے ہیں۔ ایسے سیکیورٹی سوالات منتخب کرنے کو یقینی بنائیں، جن کے جوابات صرف آپ کو ہی معلوم ہوں۔ آپ سیکیورٹی سوالات کے لیے اپنے جوابات بھی تیار کر سکتے ہیں، جب تک کہ آپ انہیں پاس ورڈ مینیجر میں محفوظ نہیں کرتے ہیں یا وہ یاد رکھنے میں آسان ہوتے ہیں۔

ویب سائٹس فون نمبر یا صارف کے اکاؤنٹ سے وابستہ ای میل کا استعمال کر کے صارفین سے رابطہ کر سکتی ہیں۔ اگر صارف اپنا پاس ورڈ بھول جاتا ہے تو ویب سائٹس اکثر ایک عارضی پاس ورڈ یا ہائپر لنک فراہم کرتی ہیں، جسے صارف اپنا پاس ورڈ ری سیٹ کرنے کے لیے استعمال کر سکتے ہیں۔

اپنے طلباء سے پوچھیں

کیا یہ اس بات کو یقینی بنانے کا محفوظ طریقہ ہے کہ نئے پاس ورڈ کی درخواست کرنے والا شخص ہی صارف ہے؟

اگر آپ اکاؤنٹ سے وابستہ ای میل پتہ کا اشتراک کرتے ہیں تو کیا ہوتا ہے؟

1. پاس ورڈ ری سیٹ کرنے کا لنک کا طریقہ زیادہ تر محفوظ ہوتا ہے، لیکن اگر آپ اکاؤنٹ یا پاس ورڈ کا کسی اور کے ساتھ اشتراک کرتے ہیں تو اس سے آپ کے لیے خطرہ لاحق ہو جاتا ہے۔

اپنے طلباء کو بتائیں

وہ لوگ سوشل چیکنگ کر سکتے ہیں جو براہ راست آپ سے رابطہ کر رہے ہوتے ہیں اور آپ سے آپ کی معلومات حاصل کرنے کی کوشش کر رہے ہوتے ہیں۔ کبھی کبھی، لوگ آپ کو کچھ اور بن کر ای میل

کریں گے (جیسے کہ دوست، فیملی کے رکن، یا بینک کی طرف سے کوئی فرد) اور آپ کی شناخت کی توثیق کرنے کے لیے آپ سے اہم معلومات کا اشتراک کرنے کو کہیں گے (جیسے کہ آپ کی تاریخ پیدائش)۔ اس کا پتا لگانا اور بھی مشکل ہو سکتا ہے۔ جیسے کہ اگر کسی شخص نے آپ کے دوست کے سوشل میڈیا اکاؤنٹ کو حیک کر لیا ہے اور آپ کو (اور ممکنہ طور پر کئی دیگر لوگوں کو بھی) پیغام بھیجتا ہے اور آپ سے آپ کی تاریخ پیدائش یا آپ کے بڑے ہونے کا مقام معلوم کرتا ہے۔ اگر آپ کو کسی ایسے دوست سے پیغامات موصول ہوتے ہیں جو آپ کو عجیب لگتا ہے تو ممکن ہے کہ آپ اس کی وضاحت کرنے کے لیے کہ واقعی آپ کا دوست مواد بھیج رہا ہے آپ پہلے (سوشل میڈیا پلیٹ فارم کے علاوہ کسی دوسرے طریقے سے) اس سے رابطہ کرنا چاہیں۔

ایسے حملے کو اصل دکھائے دینے والے ای میل یا ویب سائٹ کا استعمال کرتے ہیں، انہیں فریب دہی کہا جاتا ہے اور اس میں شناخت کی معلومات چوری ہو سکتی ہے۔ مثال کے طور پر، شناخت کی چوری سے آپ کے نام پر کریڈٹ کارڈز بنوائے جا سکتے ہیں اور ان کا استعمال کیا جا سکتا ہے، جس کی وجہ سے آپ کے بوٹھے ہونے پر آپ کے لیے کریڈٹ کارڈ بنوانا مشکل ہو سکتا ہے۔

فریب دہی کے ذریعے چور آپ کی جگہ لے سکتا ہے اور آپ کی معلومات تک رسائی حاصل کر سکتا ہے، اس سے اسے خفیہ طریقے سے آپ کے ای میلز تک پہنچنے، آپ کی طرف سے آپ کے دوستوں کو پیغام بھیجنے یا آپ کا پیسہ چوری کرنے میں مدد ملتی ہے۔ اس کے ذریعے چور ایک ایسا نیا پاس ورڈ بنا کر جو آپ کو نہ معلوم ہو، آپ کو آپ کے اکاؤنٹ سے مسدود بھی کر سکتا ہے۔

اسائمنٹ

ہینڈ آؤٹ

اسائمنٹ

شرکاء سے مندرجہ ذیل سوالات کے جواب دینے اور ان کے جوابات کو متن یا بصری وسائل کی شکل میں پاس ورڈ کے متعلق جانتے کے ہینڈ آؤٹ میں شامل کرنے کو کہیں۔

1. اس سیشن کی وہ تین بصیرتیں کون سی ہیں جو آپ کو اگلی بار پاس ورڈ بنانے کی ضرورت ہونے پر آپ لاگو کریں گے؟
2. ایک ایسی مثال کیا ہے جہاں آپ محسوس کرتے ہیں کہ کسی اور کے ساتھ اپنے پاس ورڈ کا اشتراک کرنا ٹھیک ہے؟
3. کسی اور شخص کے ساتھ محفوظ طریقے سے آپ کے پاس ورڈ کا اشتراک کرنے کے لیے تین حکم عملی کون سی ہیں جن کا آپ استعمال کر سکتے ہیں؟
4. اگر آپ کا پاس ورڈ غلط ہاتھوں میں چلا جائے تو اس کے نتیجے میں جو غلط ہو سکتا ہے اس کی تین مثالیں کیا ہیں؟