اکتوبر 2024

سائبر سیکیورٹی سے آگاہی کا مہینہ

خود کو محفوظ رکھیں!

1. **جعل سازی (phishing) ای میلز سے خبردار رہیں**
جعل سازی (Phishing) اس وقت ہوتی ہے جب سائبر جرائم پیشہ افراد جعلی ای میلز کے ذریعے معلومات چوری کرنے کی کوشش کرتے ہیں۔ یہ اپنے آپ کو کوئی اور فرد ظاہر کرتے ہیں اور چاہتے ہیں کہ آپ خطرناک لنکس پر کلک کریں۔ اگر کوئی ای میل مشکوک لگتا ہے تو محتاط رہیں ، چیک کریں کہ اسے کس نے بھیجا ہے اور کیا ان کا ای میل پتہ اس بات کی تصدیق کرتا ہے کہ بھیجنے والا وہی ہے جو وہ بتا رہا ہے۔

2. **ملٹی فیکٹر تصدیق (Multi-Factor Authentication (MFA)) کا استعمال کریں**
جب آپ MFA کے ساتھ لاگ اِن ہو رہے ہوں تو ہیکرز (سائبر چور) کے خلاف دفاع کی ایک اضافی تہہ حاصل کریں۔ یہ ایک خفیہ کوڈ کے ساتھ ایک ٹیکسٹ کی طرح ہے جس کی معیاد ایک مرتبہ استعمال کرنے کے بعد ختم ہو جاتی ہے۔

3. **مشکل پاس ورڈ یا پاس فریز استعمال کریں**
ہر جگہ ایک ہی پاس ورڈ استعمال نہ کریں! حروف، ہندسے اور علامات کا استعمال کریں۔ (پاس ورڈ) جتنا طویل ہو گا اتنا ہی بہتر ہوگا، اور پاس فریز مدد کر سکتے ہیں۔

4. **اپنے سافٹ ویئر کو جدید ترین (اپ ٹو ڈیٹ) رکھیں**
یہ سائبر چوروں کے ڈالے گئے سافٹ ویئر سے انفیکشن کے خطرے کو کم کرتا ہے جو آپ کی معلومات چوری کرسکتا ہے یا آپ کے کمپیوٹر میں وائرس پھیلا سکتا ہے۔

5. **ہوشیار رہیں، سوشل میڈیا پر محفوظ رہیں!**
آپ کی مکمل تاریخِ پیدائش، گھر کا پتہ، یا آپ کی موجودگی کا مقام، جیسی ذاتی معلومات کو آپ کی شناخت کو چوری کرنے یا غنڈہ گردی کرنے کے لیے استعمال کیا جا سکتا ہے۔

6. **شیلڈز اپ – محفوظ وائی فائی استعمال کریں**
پبلک نیٹ ورکس غیر محفوظ ہوتے ہیں۔ کوئی بھی بشمول ای میل اور یا بینک اکاؤنٹ میں لاگ ان ہونے کے، یہ دیکھ سکتا ہے کہ آپ آن لائن کیا کر رہے ہیں ۔

7. **مصنوعی ذہانت (AI) سے چلنے والی جعل سازی سے آگاہ رہیں**
سائبر جعلساز حقیقت پسندانہ تصاویر ، متن ، آواز اور ویڈیو بنانے کے لئے جدید مصنوعی ذہانت (AI)کا استعمال کرتے ہیں۔ اس سے جعلسازی اور دیگر فراڈ کا پتہ لگانا مشکل ہو جاتا ہے۔ کسی بھی غیر متوقع مواصلات پر بھروسہ کرنے سے پہلے محتاط رہیں اور ہمیشہ دوبارہ چیک کریں (بھیجنے والے کی تصدیق کریں ، مصنوعی ذہانت (AI) ہونے کی نشانیاں جیسے تاکیدی زبان ، غیر فطری آوازیں ، یا قدرے مسخ شدہ تصاویر پر نظر رکھیں۔)