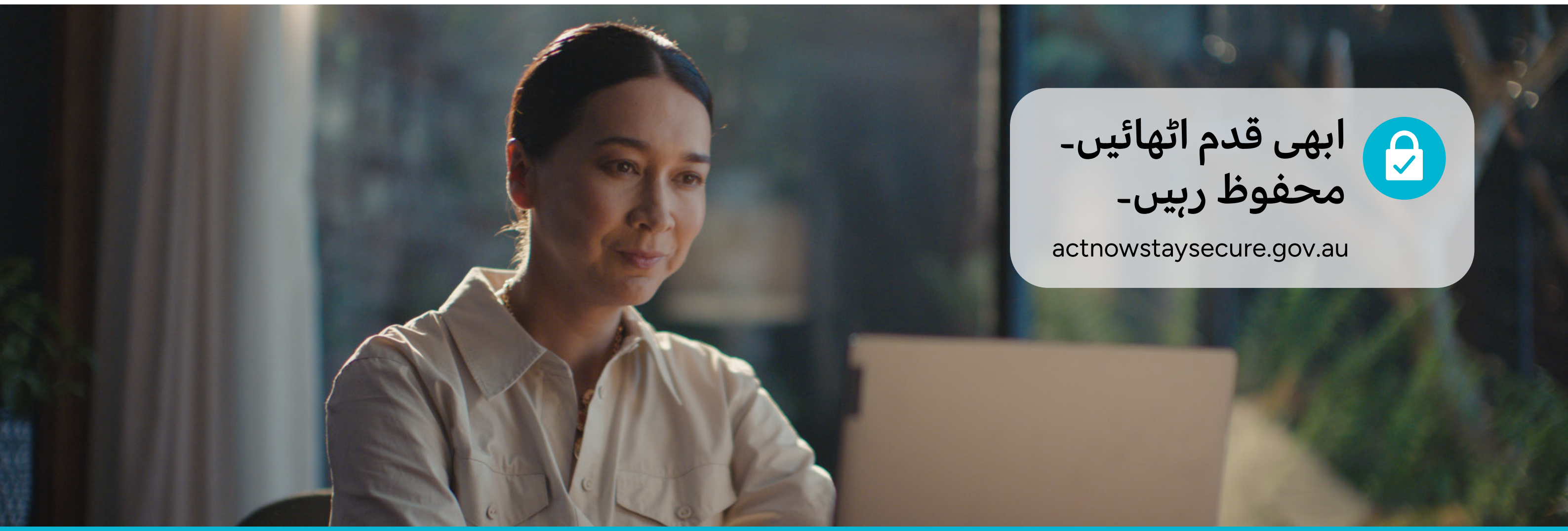
Australian Government

actnowstaysecure.gov.au



آپ کو آن لائن کونسے خطرات پیش ہوتے ہیں؟

ٹیکنالوجی کی تیزی سے ترقی اور ہمارے زیادہ وقت آن لائن گزارنے کے ساتھ ساتھ، آسٹریلیا کے لوگ سائبر حملوں کے خطرے سے دوچار ہیں۔

'ابھی قدم اٹھائیں۔ محفوظ رہیں۔' مہم آسٹریلیا کے لوگوں کو سائبر حملوں سے محفوظ رہنے کے آسان طریقوں کے متعلق آگہی دیتی ہے جن کے ذریعے ہر شخص خود کو آن لائن محفوظ رکھ سکتا ہے۔

ابھی قدم اٹھائیں۔ محفوظ رہیں۔

ہم کیسے آن لائن محفوظ رہ سکتے ہیں

اپنے ہر اکاؤنٹ کے لیے منفرد اور سٹرانگ پاس فریز (passphrase) استعمال کریں

اپنے ہر آن لائن اکاؤنٹ کے لیے منفرد اور سٹرانگ پاس فریز استعمال کرنا ان مؤثر ترین کاموں میں شامل ہے جو آپ آن لائن محفوظ رہنے کے لیے کر سکتے ہیں۔

پاس فریز سے مراد زیادہ سیکیور پاس ورڈ ہے۔ اس میں مختلف اتفاقیہ الفاظ کا ایک سلسلہ ہوتا ہے۔ پاس فریز کو یاد رکھنا آپ کے لیے آسان ہوتا ہے لیکن سائبر مجرموں کے لیے اندازے سے اسے معلوم کرنا مشکل ہوتا ہے۔

اپنے پاس فریزز کو سٹرانگ اور منفرد بنانے کے لیے، ضرور خیال رکھیں کہ ان میں:

- ✓ چار یا چار سے زیادہ اتفاقیہ چنے ہوئے الفاظ ہوں
- ✓ 15 یا اس سے زیادہ کیریکٹرز ہوں
- ✓ ہر اکاؤنٹ کے لیے مختلف پاس فریز ہو
- ✓ اپنی شناخت کروانے والی معلومات شامل نہ کریں جیسے فیملی نیم، تاریخ پیدائش یا پتہ
- ✓ اگر ویب سائیٹ یا سروس آپ کے پاس فریز میں سمبلز، کیپیٹل حروف یا ہندسے شامل کرنے کا تقاضا کرتی ہو تو یہ شامل کریں۔

اپنے منفرد پاس فریزز بنانے اور محفوظ رکھنے کے لیے پاس ورڈ مینیجر استعمال کرنے پر غور کریں۔

اپنی ڈیوائسز کو محفوظ رکھنے کے لیے تمام سافٹ ویئر اپ ڈیٹس انسٹال کریں

اپنی انٹرنیٹ سے کنیکٹڈ تمام ڈیوائسز (جیسے فون، لیپ ٹاپ یا سمارٹ واچ) کے لیے ہمیشہ سافٹ ویئر اپ ڈیٹس انسٹال کرنا خود کو آن لائن محفوظ رکھنے کے لیے نہایت اہم ہے۔

سافٹ ویئر اپ ڈیٹس آپ کی ڈیوائسز کی سیکیورٹی میں کمزوریوں یا نقائص کو ٹھیک کرتی ہیں۔ باقاعدگی سے اپ ڈیٹس انسٹال کرتے رہنے سے آپ کی ڈیوائسز محفوظ رہیں گی اور سائبر مجرموں کے لیے ان تک پہنچنا مشکل ہو جائے گا۔

آٹو میٹک اپ ڈیٹس کو آن کر دیں اور جب ڈیوائس اپ ڈیٹ انسٹال کرنے کے لیے پوچھے تو ضرور انسٹال کریں۔

ہمیشہ ملٹی فیکٹر آتھینٹیکیشن استعمال کریں

جہاں ملٹی فیکٹر آتھینٹیکیشن دستیاب ہو، اسے آن کر لیں تاکہ آپ کے تمام آن لائن اکاؤنٹس کو سکیورٹی کی ایک اور تہ مل جائے۔

ملٹی فیکٹر آتھینٹیکیشن میں آپ کو اپنے اکاؤنٹ میں لاگ ان کرنے کے لیے دو یا دو سے زیادہ ویریفیکیشن کے طریقے استعمال کرنے پڑتے ہیں۔ مثال کے طور پر، پاس ورڈ یا پاس فریز اینٹر کرنے کے بعد، آپ سے ایک اور ویریفیکیشن مانگی جائے گی جیسے آتھینٹیکیشن ایپ، ای میل یا ٹیکسٹ کے ذریعے بھیجا گیا کوڈ۔

ملٹی فیکٹر آتھینٹیکیشن آپ کے اکاؤنٹ کو تب بھی محفوظ رکھتی ہے جب دوسرے آتھینٹیکیشن کے طریقوں (جیسے پاس فریز) کو ناکام بنا دیا جائے۔

کیا آپ آن لائن محفوظ رہنے کے مزید طریقے جاننا چاہتے ہیں؟

کیا آپ سائبر سیکیور رہنے کے مزید طریقے تلاش کر رہے ہیں؟ یہاں کچھ دوسرے کام بتائے جا رہے ہیں جن کے ذریعے آپ خود کو آن لائن محفوظ رکھ سکتے ہیں۔

پبلک وائی فائی استعمال کرتے ہوئے محتاط رہیں

پبلک وائی فائی استعمال کرتے ہوئے اپنی کوئی حسّاس یا پرائیویٹ تفصیلات نہ کھولیں کیونکہ یہ کنیکشن سیکیور نہیں ہوتا۔
اس میں آپ کے سوشل میڈیا، ای میل اور آن لائن بینکنگ شامل ہیں۔ آپ یہاں جو بھی معلومات اینٹر کریں گے، وہ سائبر مجرموں کے ہاتھ لگ سکتی ہیں۔

اپنی پرائیویسی اور لوکیشن سیٹنگز کو باقاعدگی سے چیک اور اپ ڈیٹ کرتے رہیں

اکثر اپنی پرائیویسی اور لوکیشن سیٹنگز کو چیک کرتے رہنا یہ یقینی بنانے کے لیے اہم ہے کہ آپ غلطی سے اپنی ذاتی تفصیلات اور شناخت کروانے والی تفصیلات کو لوگوں کے ساتھ شیئر نہ کر دیں۔

جن سیٹنگز کو چیک کرنا ضروری ہے، ان میں آپ کے سوشل میڈیا اکاؤنٹس کی پرائیویسی سیٹنگز اور آپ کی ایپس اور ڈیوائسز پر جیو لوکیشن ٹریکنگ شامل ہیں۔

اپنے دوستوں اور گھر والوں کے ساتھ سائبر سیکیور رہنے کے طریقوں پر بات کریں

آپ، آپ کے گھر والوں اور دوستوں کے آن لائن محفوظ رہنے کے لیے یہ نہایت اہم ہے کہ سب کو معلومات اور آگہی حاصل ہو – خاص طور پر اگر آپ انٹرنیٹ سے کنیکٹڈ ڈیوائسز مل کر استعمال کرتے ہوں تو۔ اپنے قریبی لوگوں سے اس بارے میں بات کرنے سے سب کو سائبر سیفٹی کا خیال رہتا ہے اور یہ یقینی ہوتا ہے کہ انہیں خود کو آن لائن محفوظ رکھنے کے لیے تازہ ترین معلومات مل رہی ہیں۔

دھوکے بازی کو پہچاننا سیکھیں

دھوکے باز مجرم لوگوں کو جھانسا دے کر ان سے پیسے یا ان کی ذاتی تفصیلات ہتھیا لیتے ہیں۔

اگر آپ کو یقین سے معلوم نہ ہو کہ آپ کا واسطہ کس سے ہے تو کبھی کسی کو پیسے یا ذاتی تفصیلات نہ دیں۔ خود آفیشل ویب سائیٹ یا ایپ سے متعلقہ شخص یا تنظیم کی تفصیلات حاصل کر کے رابطہ کریں۔

سائبر حملوں اور واقعات کی رپورٹ کریں

سائبر حملوں اور واقعات کی رپورٹ کرنا گورنمنٹ کو نئے رجحانات کا پتہ چلانے اور کمیونٹی کو خبردار کرنے میں مدد دینے کے لیے اور سائبر واقعات کے بعد آپ کو سنبھلنے میں مدد دینے کے لیے نہایت اہم ہے۔

actnowstaysecure.gov.au پر وہ آسان طریقے سیکھیں جن سے آپ خود کو محفوظ رکھ سکتے ہیں۔

ابھی قدم اٹھائیں۔
محفوظ رہیں۔
actnowstaysecure.gov.au