Australian Government

ابھی قدم اٹھائیں۔ محفوظ رہیں۔

آن لائن محفوظ رہنے کے طریقے

آسان ورژن

Easy Read

اس گائیڈ کو کیسے استعمال کریں

ہم آسٹریلوی حکومت ہیں۔

ہم نے یہ گائیڈ بنائی ہے۔

ہم نے کچھ الفاظ **موٹے** حروف میں لکھے ہیں۔

ہم ان الفاظ کی وضاحت کرتے ہیں۔

ان الفاظ کی فہرست صفحہ 28 پر موجود ہے۔

آپ کسی قابلِ اعتماد شخص سے مدد مانگ سکتے ہیں تا کہ آپ:

- یہ گائیڈ پڑھ سکیں
- مزید معلومات ڈھونڈ سکیں۔

یہ ایک اور گائیڈ کا آسان خلاصہ ہے۔

اس میں صرف اہم ترین باتیں شامل ہیں۔

آپ وہ دوسری گائیڈ ہماری ویب سائٹ پر دیکھ سکتے ہیں۔

www.actnowstaysecure.gov.au

اس گائیڈ میں کیا شامل ہے؟

اس گائیڈ میں کیا شامل ہے؟	3
اس گائیڈ کے بارے میں	4
اپنے اکاؤنٹس کو محفوظ رکھیں	6
اپنی معلومات کی حفاظت کے لیے سیٹنگز چیک کریں	10
اپنی ڈیوائیسز کی حفاظت کریں	16
دھوکہ دہی یا سکیم (Scams)	20
آواز اٹھائیں	25
الفاظ کی فہرست	28
ہم سے رابطہ کریں	30

اس گائیڈ کے بارے میں

ہم سب کو یہ سوچنا چاہیے کہ ہم آن لائن محفوظ کیسے رہ سکتے ہیں۔

ہم اس کو **سائبر** سیفٹی کہتے ہیں۔

سائبر کا مطلب ہے کہ کوئی چیز انٹرنیٹ سے متعلق ہے۔

یہ گائیڈ بتاتی ہے کہ آپ آن لائن خود کو کیسے محفوظ رکھ سکتے ہیں۔

مثلاً **سائبر کرائم** سے بچنے کے طریقے۔

سائبر کرائم یہ ہوتا ہے جب مجرم انٹرنیٹ کو جرم کے لیے استعمال کریں۔

مثلاً وہ انٹرنیٹ کو درج ذیل کے لیے استعمال کریں:

- آپ کی ذاتی تفصیلات چرانا
- آپ کے آن لائن اکاؤنٹس یا پروفائلز پر قبضہ کرنا۔

سائبر کرائم کسی بھی ڈیوائیس پر ہو سکتا ہے۔

اس میں یہ شامل ہیں:

- کمپیوٹر
- سمارٹ فون
- سمارٹ واچ۔

سائبر کرائم سے محفوظ رہنے کے لیے آپ کچھ اقدامات کر سکتے ہیں۔

اگلے صفحات پر ہم بتائیں گے کہ آپ کیا کر سکتے ہیں۔

اپنے اکاؤنٹس کو محفوظ رکھیں

آپ کو سوچنا چاہیے کہ آپ اپنے آن لائن اکاؤنٹس کو کیسے محفوظ رکھ سکتے ہیں۔

مضبوط اور الگ الگ پاس فریز استعمال کریں

پاس فریز پاس ورڈ سے زیادہ مضبوط ہوتا ہے۔

دوسرے لوگوں کے لیے اسے اندازے سے معلوم کرنا بہت مشکل ہوتا ہے۔

مضبوط اور ہر اکاؤنٹ کے لیے الگ پاس فریز استعمال کرنا آپ کے اکاؤنٹس کی حفاظت کے بہترین طریقوں میں سے ایک ہے۔

آپ کو اپنے ہر آن لائن اکاؤنٹ کے لیے ایک الگ پاس فریز استعمال کرنا چاہیے۔

مضبوط پاس فریز میں یہ چیزیں شامل ہوتی ہیں:

- 4 یا اس سے زیادہ بے تعلق/اتفاقیہ الفاظ
- 15 یا اس سے زیادہ حروف اور نمبر۔

آپ کچھ بڑے حروف (capital letters) شامل کر سکتے ہیں۔

آپ خاص علامات (symbols) بھی استعمال کر سکتے ہیں جیسے:

- ڈیش (-)
- ڈالر کا نشان ($)
- ای میل کا @ نشان۔

آپ کو اپنے پاس فریز میں کوئی ذاتی تفصیلات نہیں ڈالنی چاہیئں۔

مثلاً:

- آپ کی تاریخ پیدائش
- آپ کے خاندان کے افراد یا پالتو جانوروں کے نام۔

اپنے اکاؤنٹس میں لاگ ان کے لیے اضافی طریقے شامل کریں

آپ **ملٹی فیکٹر آتھنٹیکیشن (MFA)** سے اپنے آن لائن اکاؤنٹس کو محفوظ کر سکتے ہیں۔

MFA کا مطلب ہے کہ ہر بار لاگ ان کرتے وقت آپ 2 یا اس سے زیادہ مختلف طریقے استعمال کریں۔

مثلاً پہلے آپ اپنا پاس فریز داخل کریں۔

پھر ایک کوڈ جو آپ کو اپنے فون پر ملتا ہے۔

آپ ان طریقوں میں سے کوئی طریقہ چن سکتے ہیں:

- فون پر ایک ایپ سے کوڈ حاصل کریں

- ای میل پر کوڈ حاصل کریں

- ٹیکسٹ میسج پر کوڈ حاصل کریں۔

MFA سے دوسرے لوگوں کے لیے آپ کے آن لائن اکاؤنٹس میں داخل ہونا مشکل بنا دیتا ہے۔

چاہے انہیں آپ کا پاس فریز معلوم ہو جائے۔

اپنی معلومات کی حفاظت کے لیے سیٹنگز چیک کریں

آپ چیک کر سکتے ہیں کہ آپ کی سیٹنگز آن لائن آپ کی معلومات کی حفاظت کر رہی ہیں یا نہیں۔

اس میں یہ سیٹنگز شامل ہیں:

- آن لائن اکاؤنٹس
- ڈیوائیسز
- ایپس۔

آپ یہ کر سکتے ہیں:

- اپنی سیٹنگز تبدیل کریں
- چنیں کہ کون سی ایپس آپ کی معلومات استعمال کر سکتی ہیں۔

آپ اپنی ڈیوائیس پر سیٹنگز اس طرح ڈھونڈ سکتے ہیں:

- گیئر (⚙) کا آئیکن تلاش کریں

یا

- یا اپنی ڈیوائیس کے سرچ (search) فنکشن میں 'settings' ٹائپ کریں

آپ کسی ایپ یا آن لائن اکاؤنٹ میں مینو کو کھول کر سیٹنگز تلاش کر سکتے ہیں۔

اکثر تین سیدھی لکیریں مینو کی علامت کے طور پر استعمال کی جاتی ہیں۔

کچھ سیٹنگز آپ کے بارے میں یہ معلومات شیئر کر سکتی ہیں :

- آپ کون ہیں
- آپ کہاں ہیں
- آپ کہاں رہتے ہیں۔

آن لائن یہ معلومات شیئر کرنا آپ کو سائبر کرائم کا نشانہ بنا سکتا ہے۔

سائبر مجرم آپ کی تفصیلات استعمال کر کے آپ کے نام سے جرم کر سکتے ہیں۔

مثلاً وہ ان معلومات کا غلط استعمال کر سکتے ہیں جیسے کہ:

- آپ کہاں رہتے ہیں

- آپ کے خاندان کے افراد کے نام

- آپ کے پالتو جانوروں کے نام۔

آپ اپنے اکاؤنٹس کو اس طرح سیٹ کر سکتے ہیں کہ صرف آپ کے جاننے والے ہی آپ کے سوشل میڈیا پروفائلز دیکھ سکیں۔

مثلاً آپ کا فیس بک پروفائل۔

یہ سیٹنگز عموماً 'پرائیویسی سیٹنگز' کہلاتی ہیں۔

آپ اپنی **لوکیشن سیٹنگز** بھی کنٹرول کر سکتے ہیں۔

لوکیشن سیٹنگز یہ ظاہر کرتی ہیں کہ آپ کی ڈیوائیس کہاں ہے۔

آپ انہیں آن یا آف کر سکتے ہیں

آپ یہ بھی چن سکتے ہیں کہ کون سی ایپس لوکیشن سیٹنگز استعمال کر سکتی ہیں۔

آپ یہ ان کے لیے کر سکتے ہیں:

- آن لائن اکاؤنٹس
- ڈیوائیسز
- ایپس۔

کچھ ایپس یہ بھی اجازت مانگ سکتی ہیں:

- آپ کا کیمرہ استعمال کریں

- آپ کی تصویریں دیکھیں۔

آپ کو صرف ان ایپس کو کیمرہ اور تصویریں استعمال کرنے کی اجازت دینی چاہیے جن سے آپ واقف ہوں۔

اپنی ڈیوائیسز کی حفاظت کریں

آپ کو سوچنا چاہیے کہ آپ اپنی ڈیوائیسز کو آن لائن کیسے محفوظ رکھ سکتے ہیں۔

مثلاً آپ کا فون یا اسمارٹ واچ۔

یہ ان ڈیوائیسز کے لیے بہت ضروری ہے جو انٹرنیٹ سے جڑتی ہیں۔

اپنی ڈیوائیسز کو اپ ڈیٹ کریں

آپ اپنی ڈیوائیسز کو اپ ڈیٹ کر کے انہیں آن لائن محفوظ رکھ سکتے ہیں۔

مثلاً اپنا فون اور لیپ ٹاپ۔

ممکن ہے، آپ کی ڈیوائیس میں اسے سافٹ وئیر اپ ڈیٹ کہا جاتا ہو۔

اپ ڈیٹس ڈیوائیس کو سائبر کرائم سے بچانے میں مدد کرتی ہیں۔

آپ ڈیوائیس پر خودبخود اپ ڈیٹ ہونے کی سیٹنگ کر سکتے ہیں۔

آپ اپنی ڈیوائیسز کو اپ ڈیٹ کرنے کے بارے میں مزید معلومات ہماری ویب سائٹ پر دیکھ سکتے ہیں۔

www.actnowstaysecure.gov.au/cyber-safe-actions

پبلک وائی فائی نیٹ ورک

آپ کو پبلک وائی فائی استعمال کرتے وقت احتیاط کرنی چاہیے۔

پبلک وائی فائی مفت وائر لیس انٹرنیٹ ہے جو آپ عوامی مقامات پر استعمال کر سکتے ہیں۔

مثلاً:

- کیفے
- ائیر پورٹ
- یا ہوٹل میں۔

آپ کو احتیاط کرنی چاہیے کہ پبلک وائی فائی استعمال کرتے ہوئے آپ کسی ویب سائٹ پر کون سی معلومات داخل کرتے ہیں۔

مثلاً آپ کے:

- بینک کی تفصیلات
- ای میل اکاؤنٹس
- سوشل میڈیا پروفائلز۔

کچھ سائبر مجرم پبلک وائی فائی کو استعمال کر کے:

- آپ کی آن لائن سرگرمی دیکھ سکتے ہیں
- آپ کی معلومات چرا سکتے ہیں۔

کیونکہ:

- کوئی بھی پبلک وائی فائی کو استعمال کر سکتا ہے

اپنی ڈیوائیسز کو محفوظ رکھنا زیادہ مشکل ہوتا ہے۔

آپ ہماری ویب سائٹ پر ہبلک وائی فائی استعمال کرتے ہوئے محفوظ رہنے کے طریقے جان سکتے ہیں۔

www.actnowstaysecure.gov.au/cyber-safe-actions

دھوکہ دہی یا سکیم (Scams)

ہم اسے **سکیم** کہتے ہیں جب کوئی:

- آپ کو دھوکہ دینے کی کوشش کرے
- آپ کے پیسے ہتھیانے کی کوشش کرے۔

سکیمر وہ شخص ہوتا ہے جو دھوکا یا فراڈ کرتا ہے۔

سکیمر آپ کو ان ذریعوں سے دھوکہ دینے کی کوشش کر سکتے ہیں:

- ٹیکسٹ میسج یا فون کال
- ای میل
- سوشل میڈیا
- ویب سائٹ۔

ان کا رویہ دوستانہ لگ سکتا ہے۔

لیکن ممکن ہے، وہ دھوکے سے آپ سے آپ کی تفصیلات حاصل کرلیں۔

وہ ان معلومات کو یہ کرنے کے لیے استعمال کر سکتے ہیں:

- آپ کے آن لائن اکاؤنٹس میں داخل ہوں

- آپ کا نام استعمال کر کے جرم کریں

- آپ کے پیسے چرائیں۔

سکیمر یہ بھی کر سکتے ہیں:

- آپ کو دھوکہ دینے کے لیے جھوٹے اکاؤنٹس بنائیں

- آپ لنکس اور اشتہار بھیج کر ان پر کلک کرنے کے لیے کہیں ۔

سکیم کو کیسے پہچانیں؟

یہ ایک سکیم ہو سکتا ہے اگر کوئی:

- آپ کو فوراً کچھ کرنے کو کہے

- آپ کو بہت سے پیسے دینے کی پیشکش کرے

- آپ سے پیسے مانگے

- آپ کو کسی لنک پر کلک کرنے کو کہے۔

سکیمر کسی ایسی تنظیم کا روپ دھار سکتے ہیں جس پر آپ بھروسہ کرتے ہیں۔

مثلاً آپ کا بینک۔

وہ ایسا اس لیے کرتے ہیں تاکہ آپ انہیں اپنی ذاتی معلومات دے دیں۔

اگر آپ کو کسی شخص کے بارے میں لگے کہ وہ سکیمر ہے تو اس سے بات کرنا بند کریں۔

آپ کو چیک کرنا چاہیے کہ وہ شخص اپنے بارے میں واقعی سچ بتا رہا ہے۔

آپ اس شخص یا تنظیم سے رابطہ کر سکتے ہیں جس کی تفصیلات بھروسے کے لائق ہوں اور آپ نے خود ڈھونڈی ہوں۔

اگر کچھ غلط لگے تو فوری طور پر خود کو بچانے کے اقدامات کریں۔

سکیم کو رپورٹ کرنا

Scamwatch آسٹریلوی لوگوں کی مدد کرتا ہے:

- سکیموں کو سمجھنے میں
- سکیموں کو رپورٹ کرنے میں۔

Scamwatch سکیم کا سامنا کرنے والوں کی بھی مدد کرتا ہے۔

آپ Scamwatch ویب سائٹ پر سکیم کو رپورٹ کر سکتے ہیں۔

www.scamwatch.gov.au/report-a-scam

آواز اٹھائیں

آپ کو اس بارے میں بات کرنی چاہیے کہ دوسرے لوگ آن لائن خود کو کیسے محفوظ رکھ سکتے ہیں۔

اس میں یہ شامل ہے:

- سائبر کرائم کو رپورٹ کرنا

- گھر والوں اور دوستوں کے ساتھ اپنا علم شیئر کرنا۔

ہم اگلے صفحات میں بیان کریں گے کہ آپ کیسے آواز اٹھا سکتے ہیں۔

سائبر کرائم کو رپورٹ کریں

سائبر کرائم کو رپورٹ کرنے سے حکومت کو اس میں مدد ملتی ہے:

- یہ جاننا کہ سائبر مجرم لوگوں پر کیسے حملہ کرنے کی کوشش کرتے ہیں

- زیادہ لوگوں کی حفاظت کرنا۔

آپ ReportCyber ویب سائٹ پر سائبر جرم کی اطلاع دے سکتے ہیں.

www.cyber.gov.au/report

گھر والوں اور دوستوں سے آن لائن محفوظ رہنے کے بارے میں بات کریں

آپ کو آن لائن محفوظ رہنے کے اپنے مشورے اپنے گھر والوں اور دوستوں کے ساتھ شیئر کرنے چاہئیں۔

آپ ان سے بھی سیکھ سکتے ہیں۔

آن لائن محفوظ رہنے کے بارے میں اپنا علم شیئر کر کے آپ اپنے اور اپنے آس پاس کے لوگوں کی حفاظت کر سکتے ہیں۔

یہ خاص طور پر تب اہم ہے اگر آپ دوسروں کے ساتھ ڈیوائیسز شیئر کرتے ہیں۔

الفاظ کی فہرست

یہ فہرست اس گائیڈ میں **موٹے** حروف میں لکھے گئے الفاظ کی وضاحت کرتی ہے۔

سائبر

سائبر کا مطلب ہے کہ کوئی چیز انٹرنیٹ سے متعلق ہے۔

سائبر کرائم

سائبر کرائم وہ ہوتا ہے جب مجرم انٹرنیٹ کو جرم کے لیے استعمال کریں۔

مثلاً انٹرنیٹ کے استعمال کے ذریعے:

- آپ کی ذاتی معلومات چرانا
- آپ کے آن لائن اکاؤنٹس پر قبضہ کرنا۔

لوکیشن سیٹنگز

لوکیشن سیٹنگز یہ ظاہر کرتی ہیں کہ آپ کی ڈیوائیس کہاں ہے۔

ملٹی فیکٹر آتھنٹیکیشن (MFA)

MFA کا مطلب ہے کہ ہر بار لاگ ان کرتے وقت آپ 2 یا اس سے زیادہ مختلف طریقے استعمال کریں۔

پاس فریز

پاس فریز پاس ورڈ سے زیادہ مضبوط ہوتا ہے۔

دوسرے لوگوں کے لیے اسے اندازے سے معلوم کرنا بہت مشکل ہوتا ہے۔

پبلک وائی فائی

پبلک وائی فائی مفت وائر لیس انٹرنیٹ ہے جو آپ عوامی مقامات پر استعمال کر سکتے ہیں۔

دھوکہ دہی یا سکیم (Scams)

ہم اسے سکیم کہتے ہیں جب کوئی:

- آپ کو دھوکہ دینے کی کوشش کرے
- آپ کے پیسے ہتھیانے کی کوشش کرے۔

سکیمر (Scammer)

سکیمر وہ شخص ہوتا ہے جو سکیم کرتا ہے۔

ہم سے رابطہ کریں

آپ آسٹریلین سائبر سیکیورٹی ہاٹ لائن پر کال کر سکتے ہیں۔

1300 292 371

آپ ہماری ویب سائٹ دیکھ سکتے ہیں۔

www.actnowstaysecure.gov.au

آپ ReportCyber ویب سائٹ پر سائبر جرم کی اطلاع دے سکتے ہیں۔

www.cyber.gov.au/report

یہ آسان یا ایزی ریڈ دستاویز Information Access Group نے تیار کی ہے جس میں اسٹاک فوٹوگرافی اور کسٹم تصاویر استعمال کی گئی ہیں۔ تصاویر کو بغیر اجازت کے دوبارہ استعمال نہیں کیا جا سکتا۔ تصاویر کے بارے میں سوالات کے لیے یہاں جائیں: www.informationaccessgroup.com ۔ جاب نمبر 6342 کا حوالہ دیں۔