Краток преглед на онлајн презентација

Australian Government

Be Connected
Every Australian online.

Дали можете да забележите измама?

Да препознавате што се измами и како тие функционираат е еден од важните чекори да ги избегнете. Секоја година повозрасните Австралијци губат милиони долари преку измами. И покрај тоа што интернетот е прекрасно место да го разгледувате и да се поврзувате со други лица, не можеме секогаш да бидеме сигурни дека луѓето се навистина тие коишто се претставуваат. Штом ќе ги знаете триковите на измамниците, тогаш е поверојатно дека ќе можете да препознаете измама.

Измами за кражба на идентитет

Измамите за кражба на идентитет се обиди на измамниците да ве излажат и да верувате дека се од некоја веродостојна организација, или лице кое го познавате, и нивната цел е да им ги дадете вашите лични податоци, како што се броеви на банкарски сметки, лозинки и броеви на кредитни картички.

Измамите за кражба на идентитет се дизајнирани да изгледаат реално и често го копираат обликот што го користи организацијата што измамникот наводно ја застапува и го вклучува нивниот бренд и лого. Овие измами може да се јават во голем број облици, вклучувајќи е-пораки, текстуални пораки или телефонски повици. На пример, може да примите:

- текстуална порака од банката што ви бара да ја потврдите вашата лозинка
- е-порака од давателот на услуги за интернет што ви бара да ги ажурирате вашите податоци
- текстуална порака од член на семејството кој користи нов телефонски број и ви бара итно да му пратите пари
- телефонски повик од вашата финансиска институција за да ве предупреди за „неовластена или сомнителна активност на вашата сметка“, или дека вашата сметка ќе се затвори ако не ги ажурирате вашите податоци
- известување на Facebook од лице кое го познавате во кое ви препорачува некоја интернет-страница.

Даночни измами и измами преку Medicare

Измамниците се претставуваат дека се од Австралиската даночна управа (Australian Tax Office - ATO), Medicare и други владини организации, за да се обидат да ве измамат да платите пари и да споделите лични податоци. Овие измамници создаваат лажни интернет-страници и ќе ви праќаат е-пораки, текстуални пораки и повици во кои ќе се претставуваат дека се од владина организација.

ATO никогаш нема да ви прати е-порака, текстуална порака или телефонски повик со кои ќе ви бара да:

- дадете лични податоци како што е вашиот даночен број, број на кредитна картичка или банкарски детали
- да платите провизија за да го примите вашиот повраток на данок, или да спречите да бидете уапсени заради затајување данок
- кликнете на некоја врска за да внесете лични податоци
- преземете датотеки или да инсталирате софтвер.

Ако не сте сигурни дали комуницирате со ATO, јавете се на бесплатната линија за помош на ATO за измами на 1800 008 540 или посетете ја ato.gov.au/scams.

Како да се заштитите

- Не брзајте. Прочитајте ја повторно пораката. Запрашајте се дали пораката или повикот би можеле да бидат лажни?
- Дали адресата на е-пошта е официјална или нешто не е како што треба?
- Кој е примателот на пораката? Ако наместо вашето име во пораката пишува „Почитуван клиенту“, тоа треба да ви биде сомнително.
- Дали содржи печатни или граматички грешки? Ова може да биде знак дека ви ја пратил некој измамник.
- Не користете ги деталите за контакт дадени во пораката бидејќи тие може да бидат лажни. Пребарајте ги на интернет телефонскиот број и официјалната интернет-страница на организацијата.
- Не кликнувајте на врски и не отворајте какви било други прилози, бидејќи тие може да преземат вирус на вашиот уред – едноставно притиснете го копчето за бришење.
- Не давајте ги никому вашите лични податоци, како што е даночниот број, датумот на раѓање, банкарската сметка или деталите на вашата кредитна картичка или банката.

Запомнете: измамниците може да се обидат да си играат со вашите чувства за да ве натераат да реагирате брзо и да не си дадете доволно време за да размислите внимателно за ситуацијата. Нивните тактики може да вклучуваат користење на закани или казни, може да ви велат дека некој неовластено троши пари од вашата сметка, или може да се претстави како член на вашето семејство кому му треба помош.

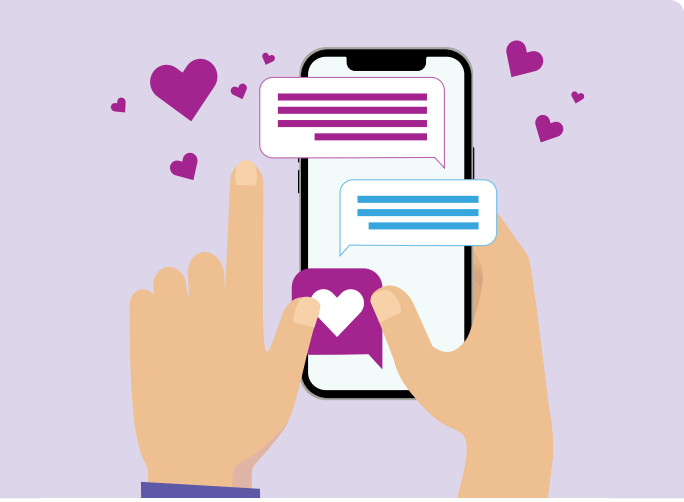
Измами преку пријателства и љубовни измами

Измамниците ги користат луѓето кои бараат пријателство или љубовна врска, често преку интернет-страници и апликации за ширење познанства, социјалните мрежи, па дури и преку онлајн игри, така што се преправаат дека се потенцијални содружници. Нивната цел е да се здобијат со вашата доверба за да им дадете пари, подароци, интимни слики или лични детали.

Што можете да направите за да бидете умешни и безбедни?

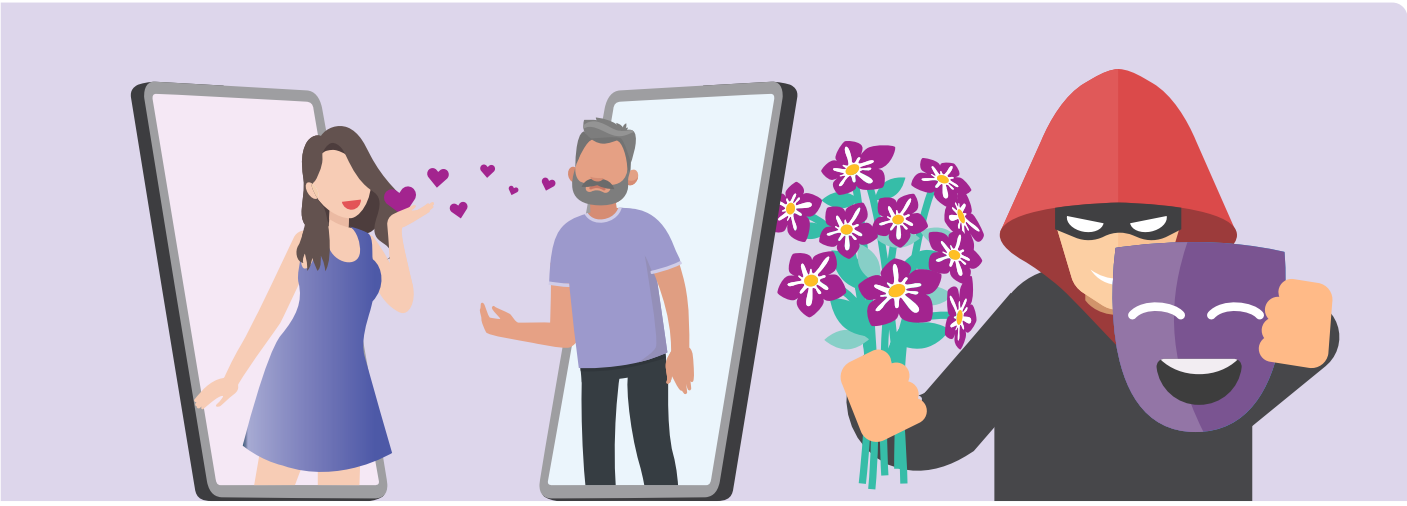
Внимавајте на луѓе кои:

- многу брзо изразуваат длабока приврзаност
- откако ќе се здобијат со вашата доверба (често чекаат недели, месеци, па дури и години), ќе ви раскажат некоја комплицирана приказна и ќе ви побараат пари или заем, подароци или податоци на вашата банкарска сметка/кредитна картичка
- избегнуваат да ве сретнат лично и даваат разни оправданија зошто не можат да патуваат за да се сретнете
- имаат онлајн-профил што не е доследен со она што ви го кажуваат за себе.



Како да се заштитите

- Никогаш не праќајте пари и не откривајте ги податоците на кредитната картичка, онлајн сметките или копии од лични документи некому кого никогаш не сте го сретнале лично.
- Извршете пребарување на фотографијата на тоа лице на Google, што може да ви помогне да утврдите дали тоа лице навистина е тој/таа што се претставува или фотографиите биле земени од друго место на интернет. Одете на images.google.com и кликнете на иконата на камера.
- Треба да почнете да се сомневате кога ќе почнат да споменуваат „проблеми со пари“ или дека им треба парична помош за „итен случај“.
- Внимавајте на печатни и граматички грешки и недоследности во приказните.
- Не споделувајте интимни слики или видеозаписи. Измамниците исто така може да ги уценуваат нивните жртви користејќи срамотен материјал.



Измами од техничка поддршка

Овие измами обично почнуваат со повик или е-пошта што доаѓа од голема телекомуникациска или компјутерска организација, на пример Telstra, NBN или Microsoft, што ве информира дека имате проблем со компјутерот или со интернетот и дека организацијата може да го поправи. Тие потоа ќе ви побараат далечински пристап до вашиот компјутер за да го „најдат проблемот“ или ќе се обидат да ве убедат да купите непотребен софтвер или услуга што ќе го „поправи“ вашиот компјутер.

Како да се заштитите

- Ако примите неочекуван телефонски повик за вашиот компјутер и ако ви побараат далечински пристап, едноставно затворете го телефонот.
- Не давајте му на несаканиот повикувач далечински пристап до вашиот компјутер.
- Не споделувајте лични информации како што се деталите на вашата банкарска сметка или кредитна картичка.
- Не купувајте софтвер што не сте го побарале преку несакан повик или е-пошта.
- Игнорирајте ги скок-пораките што ви велат да ја повикате техничката поддршка.

Совети за избегнување измами

Запрете

- Не брзајте да дадете пари или лични податоци на кое било лице.
- Измамниците ќе ви понудат да ви помогнат или ќе ви побараат да го потврдите вашиот идентитет. Тие ќе се претставуваат дека се од некоја организација што ја познавате или во која имате доверба, на пример, некој бизнис со кого соработувате, полиција, владина служба или служба за измами.

Размислете

- Запрашајте се дали пораката или повикот би можеле да бидат лажни?
- Никогаш не кликнувајте на врски во порака и прашајте некој доверлив пријател или семеен член што би направиле тие на ваше место. Контактирајте со бизниси или владини служби само преку деталите за контакт што се наоѓаат на нивните официјални интернет-страници или нивните безбедни апликации. Ако не сте сигурни, речете „не“, затворете го телефонот или избришете ја пораката.

Заштитете се

- Реагирајте брзо ако чувствувате дека нешто не е во ред.
- Веднаш контактирајте со банката ако загубите пари или лични податоци, или ако забележите необична активност на вашите картички или сметки. Побарајте помош од организациите како што се IDCARE и пријавете го електронското злосторство на ReportCyber. Помогнете им на други лица со пријавување на измамите на Scamwatch.

Ми треба помош, се сомневам дека некој се обидува да ме измами

Ако мислите дека сте жртва на измама, не треба да се чувствувате засрамено и да не го кажувате тоа. Постојат нешта што можете да ги преземете за да го поправите проблемот:

- Контактирајте со вашата банка или финансиска институција за да запрат да вршат секакви други плаќања на измамникот.
- Ако сте биле жртва на киберзлосторство и сте загубиле пари онлајн, можете да го пријавите тоа во полицијата преку ReportCyber или посетете ја: cyber.gov.au
- Ако сте загрижени дека вашите лични податоци биле откриени или злоупотребени, контактирајте со Австралиската служба за национален идентитет и кибер-поддршка (Australia's National Identity and Cyber Support Service - IDCARE) на 1300 432 273 или idcare.org
- Пријавете ја измамата кај ACCC преку страницата scamwatch.gov.au/report-a-scam. Ова помага да се предупредуваат луѓето за тековните измами, да се следат тенденциите и да се спречат злосторствата кога е можно.
- Информирајте ги вашите пријатели и семејството за да ги заштитите.

Запомнете: секогаш постои некој кој може да ви помогне, тоа може да бидат луѓето од cyber.gov.au или scamwatch.gov.au, технички образован пријател или семеен член, па дури и локален компјутерски клуб.

За да бидете информирани за најновите измами што треба да ги избегнете, запишете се да добивате Предупредувања за измами по е-пошта (Scamwatch email alerts).

Најдете време да ја разгледате веб-локацијата Be Connected

Be Connected е една богата веб-локација со бесплатни ресурси специјално дизајнирани да им помогнат на постарите Австралијци да се поврзат безбедно онлајн и да вршат навигација низ дигиталниот свет со самодоверба. Исто така, локацијата е корисна за семејствата и организациите во заедницата што сакаат да им помогнат на постарите лица да пристапат до сите придобивки од интернетот.

посетете ја beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

Оваа програма беше изведена од eSafety како дел од иницијативата „Be Connected".