AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Mala crna knjižica prijevara

Džepni vodič koji će vam pomoći prepoznati, izbjeći i zaštititi se od prijevara

Mala crna knjižica prijevara

Džepni vodič koji će vam pomoći prepoznati, izbjeći i zaštititi se od prijevara

ISBN 978 1 920702 00 7

Australska komisija za zaštitu tržišnog natjecanja i zaštitu potrošača (Australian Competition and Consumer Commission)
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 12/16_1129

www.accc.gov.au

Sadržaj

Uvod

Svake godine prijevare koštaju australske stanovnike, biznise i ekonomiju stotine milijuna dolara i uzrokuju emocionalni stres i patnju žrtvama i njihovim obiteljima.

Najbolji način da se zaštitite je kroz upućenost i edukaciju. Ovo novo izdanje *Male crne knjižice prijevara* vam je omogućila Australska komisija za zaštitu tržišnog natjecanja i zaštitu potrošača (ACCC), koja je ujedno i nacionalna agencija za zaštitu potrošača. Mala crna knjižica prijevara međunarodno je priznata kao važna pomoć za potrošače i male poduzetnike kako bi saznali više o prijevarama, uključujući:

- najčešće oblike prijevara od kojih se treba pripaziti
- različite načine na koje vas prevaranti mogu kontaktirati
- načine kojima se prevaranti koriste da bi vas prevarili
- znakove upozorenja
- kako se zaštititi, i
- gdje možete dobiti pomoć

Mala crna knjižica prijevara je dostupna preko interneta, na adresi www.accc.gov.au/littleblackbookofscams.

Zaštitite se—prijavite se na Scamwatch

Da biste ostali jedan korak ispred prevaranata, doznajte više na ACCC-ovoj Scamwatch internet stranici—www.scamwatch.gov.au—gdje se možete upisati za primanje besplatnih elektronskih upozorenja glede novih oblika prijevara usmjerenih protiv korisnika i malih biznisa. Scamwatch možete pratiti i preko Twittera na @scamwatch_gov ili http://twitter.com/scamwatch_gov.

Najčešći oblici prijevara koje treba izbjegavati

Svakoga se može prevariti, pa stoga svatko treba informacije o tome kako prepoznati i izbjeći prijevaru. Neki ljudi misle da su samo lakovjerne i pohlepne osobe žrtve prijevara. Međutim, istina je da su prevaranti lukavi i ako ne znate čega se trebate čuvati, možete i vi postati žrtva prijevare.

Jeste li ikada dobili ponudu koja izgleda previše dobro da bi bila istinita: možda telefonski poziv kojim se nudi da će vam popraviti računalo, ili pak prijetnju da morate vratiti novac koji ne dugujete, upozorenje od vaše banke ili davatelja telekomunikacijskih usluga o tome da postoji problem s vašim računom ili čak poziv da se "sprijateljite" ili se povežete s nekim na internetu? Prevaranti znaju kako vas izmanipulirati da bi dobili ono što žele.

Postaju sve lukaviji, kreću se ukorak s vremenom kako bi iskoristili prilike koje im pružaju nove tehnologije, novi proizvodi ili usluge ili veliki događaji, kako bi sastavili uvjerljive priče kojima će vas nagovoriti da im date svoj novac ili osobne podatke.

Međutim, zahvaljujući desecima tisuća prijava o prijevarama svake godine, ACCC organizacija je pripremila popis uobičajenih prijevara, kako bi vam otkrila tajne i taktike koje prevaranti ne žele da saznate.

Prijevare koje uključuju upoznavanje i romantične veze

Prijevare koje uključuju upoznavanje i romantične veze koštaju Australce milijune dolara svake godine i mogu uništiti i osobu i njenu obitelj..

Kako ovakve prijevare uspijevaju

Prevaranti koji iskorištavaju stranice za upoznavanje i romantične veze kreiraju lažne profile na legitimnim internet-stranicama za upoznavanje, mobilnim aplikacijama ili na društvenim mrežama poput Facebook-a koristeći fotografije i identitete češće puta ukradene od drugih osoba. Oni takve profile koriste kako bi s vama pokušali ući u vezu koja može trajati mjesecima ili čak godinama, samo da bi vam mogli uzeli novac. Prevaranti će tražiti novac za pomoć u slučaju bolesti, ozljeda, putnih troškova ili obiteljske krize. Oni su bezdušni i lagat će vam kako bi iskoristili vašu dobru dušu.

Prevaranti obično govore da se nalaze u inozemstvu i imaju izgovor zašto su tamo: npr. u vojnoj su službi, rade kao inženjeri ili se brinu za prijatelja ili rođaka. Oni nikada nisu ono za što se izdaju, a neki lukavi prevaranti mogu čak slati i male poklone. To je samo dio njihovog velikog plana da vam kasnije izvuku još više novca.

Zaštitite se

- Nikada nemojte slati novac niti davati svoje osobne podatke nekome koga znate samo preko interneta.
- Obratite pažnju da li je vaš internetski 'obožavatelj' zatražio da sa vama komunicira izvan stranice za upoznavanje ili platforme društvene mreže nakon samo nekoliko kontakata ili razgovora - to može biti prevarant.
- Izvršite pretragu slike 'obožavatelja' kako biste utvrdili je li ta osoba doista ono što tvrdi da jeste. Možete koristiti usluge pretraživanja slika kao što su Google ili TinEye.
- Budite oprezni kada dijelite intimne slike ili videozapise preko interneta. Poznato je da prevaranti ucjenjuju svoje žrtve pomoću slika ili videozapisa koje žrtve ne žele da drugi ljudi vide.

Investicijske prijevare

'Investicija bez rizika' ili prilika za nevolju?

Kako ovakve prijevare uspijevaju

Investicijske prijevare dolaze u različitim oblicima, uključujući kupnju kripto-valute, trgovanje binarnim opcijama, poslovne pothvate, mirovinske sheme, upravljana sredstva i prodaju ili kupnju dionica ili imovine. Prevaranti svoje lažne 'prilike' maskiraju profesionalnim brošurama i internet-stranicama kako bi prikrili svoje lažne operacije. Takve prijevare često počinju iznenadnim telefonskim pozivom ili e-mailom prevaranta koji nudi priliku 'koja se ne propušta', osigurava 'visoki povrat' ili nudi 'zajamčenu' priliku. Prevaranti obično operiraju iz inozemstva i nemaju australsku licencu za pružanje financijskih usluga.

Prijevare koje se koriste kompjuterskim softverima za predviđanje, zasnivaju se na obećanjima da će točno predvidjeti kretanja na tržištu dionica, rezultate konjskih utrka, sportskih događaja ili lutrije. Ti softveri su samo jedan oblik kockanja prerušen u investicije. Većina shema ili programa ne funkcionira i kupci ne mogu dobiti svoj novac natrag. U mnogim slučajevima dobavljač jednostavno nestaje.

Prijevare zasnovane na mirovinskom osiguranju nude vam rani pristup vašem mirovinskom fondu, često putem tzv. 'self-managed' superfondova, ili za pristojbu. Prevarant će vas nagovoriti da pristanete na izmišljenu priču koja će vam omogućiti da prijevremeno dođete do vašeg novca, a zatim, djelujući kao vaš financijski savjetnik, prevariti vaš mirovinski fond da vaša sredstva isplati direktno njemu. Jednom kada dobije vaš novac, prevarant vam može uzeti veliku maržu ili vas jednostavno ostaviti bez ičega.

Zaštitite se

- Nemojte dopustiti da netko na vas izvrši pritisak na donošenje odluka o svom novcu ili ulaganjima - osobito ako je takva ponuda pala s neba.
- Prije nego se odvojite od svog novca, sami provedite istraživanje o dotičnom investicijskom društvu i provjerite na stranici www.moneysmart.gov.au ima li osoba australsku licencu za pružanje financijskih usluga. Zapitajte se: ako bi neki neznanac znao tajnu kako se jednostavno zarađuje novac, zašto bi je otkrio drugim osobama?

Ako ste u dobi za umirovljenje, čuvajte se ponuda koje vam olakšavaju pristup očuvanim mirovinskim primanjima. Ako nezakonito pristupite svom mirovinskom fondu, možda ćete se suočiti sa kaznama u skladu s poreznim zakonom.

Prijevare lažnim prijetnjama i kaznama

Ako vam neko tzv. vladino tijelo ili legitimna tvrtka govori da nešto morate platiti, zastanite na trenutak, zapitajte se i provjerite.

Kako ovakve prijevare uspijevaju

Kod ovakvih oblika prijevara ne nudi se nagrada, novac ili povrat novca, ovakve prijevare se koriste prijetnjama kojima je cilj da vas preplaše i na taj način privole da im date novac. Prevarant vas može nazvati i zaprijetiti vam uhićenjem ili vam poslati poruku e-mailom u kojoj tvrdi da dugujete novac - npr. za **prekoračenje brzine**, da morate vratiti **dug poreznom uredu** ili da imate **neplaćeni račun**.

Tijekom telefonskog poziva, prevaranti na vas mogu izvršiti pritisak da odmah platite i reći vam da će vam poslati policiju ako to odbijete. Poznato je da prevaranti ciljaju na ugrožene ljude u našoj zajednici, kao što su novopridošli doseljenici. Prevaranti se pretvaraju da su djelatnici Odjela za imigraciju i prijete žrtvama **deportacijom**, ukoliko im se ne plati pristojba za ispravljanje grešaka u njihovim vizama. Vrlo slična prijevara uključuje prevarante koji se pretvaraju da su iz Australskog poreznog ureda i svojim žrtvama govore da imaju nepodmireni porezni račun.

Prevaranti se također pretvaraju da su **pouzdane** tvrtke, npr. vaša banka ili poduzeće za plin, struju, vodu ili telefon. Prijetit će vam da će vam otkazati uslugu ili će vam u suprotnom naplatiti iznimno visoku novčanu kaznu ako račun ne platite odmah. Oni se ponekad mogu predstavljati kao Australska pošta, s tvrdnjom da imate pošiljku koju trebate podići ili će vam se u suprotnom naplatiti pristojba za njenu pričuvu za svaki dan koji je niste podigli. U svakom slučaju, pokušavat će vas dovoljno zabrinuti da biste reagirali

bez razmišljanja i da ne biste imali vremena provjeriti je li njihova priča točna.

Ako je prijevara poslana e-mailom, vjerojatno će sadržavati privitak ili poveznicu sa lažnom internet stranicom u na kojoj će se od vas tražiti da učitate potvrdu o "računu", "novčanoj kazni" ili "pojedinostima o isporuci". Otvaranje privitka ili preuzimanje datoteke rezultirat će zaražavanjem vašeg računala zlonamjernim softverom (pogledajte stranicu 16).

Zaštitite se

- Ne dajte se ucijeniti prijetnjama preko telefona. Zastanite, razmislite i provjerite da li je njihova priča točna.
- Vladina agencija ili legitimna tvrtka nikada neće provoditi naplatu koristeći neuobičajene metode, npr. korištenjem poklon-vaučera, žičanog prijenosa Bitcoina.
- Provjerite identitet kontakta nazivajući direktno relevantnu agenciju - pronađite njihov broj kroz nezavisni izvor, npr. u telefonskom imeniku, na prethodnom računu ili pretragom preko interneta.
- nemojte koristiti kontakt-pojedinosti koje se nalaze u sumnjivom emailu ili koji su vam dani tijekom telefonskog poziva. Još jednom, pronađite ih kroz neovisne izvore.

Neočekivane novčane prijevare

Ako se od vas traži da pošaljete novac prije no što ste primili dobra ili usluge, razmislite na trenutak.

Kako ovakve prijevare uspijevaju

Prevaranti će vam iz vedra neba reći da imate pravo na novac, dragulje, zlato ili dionice, ali da biste ih dobili, morate **platiti** unaprijed. Međutim, nikada nećete dobiti ono što vam je obećano i uvijek će vam se ponuditi novi izgovor zašto morate platiti više. Ako budete plaćali njihove pristojbe, izgubit ćete novac.

Prijevare koje se koriste povratom ili potraživanjem novca govore vam da vam se duguje novac, npr. kroz preplaćeni porez, bankovnu pristojbu ili neku drugu vrstu kompenzacije. Međutim, prije nego što dobijete svoj novac, od vas će se tražiti da platite malu administrativnu pristojbu.

Kod **prijevara vezanih uz nasljeđe**, prevaranti se izdaju za odvjetnike, bankare ili strane dužnosnike i govore vam da imate pravo na veliko nasljedstvo ili da vam mogu ponuditi udio u nekom programu jer imate isto ime i prezime kao netko tko je preminuo. Oni često koriste dokumente koji izgledaju kao službeni dokumenti i traže od vas da plaćate pristojbe i poreze prije nego što dobijete nasljedstvo. Također, mogu od vas tražiti i vaše osobne podatke kako bi ispunili "službenu dokumentaciju". To znači da su vam osim novca možda ukrali i identitet.

Takozvane **nigerijske prijevare** su najvjerojatnije počele u zapadnoj Africi, ali mogu doći s bilo kojeg mjesta na svijetu. One uključuju prevarante koji vam govore da trebaju vašu pomoć kako bi osigurali 'veliko bogatstvo koje očajnički pokušavaju prebaciti iz svoje zemlje'. Oni mogu tvrditi da je njihovo bogatstvo skrivena zaliha novca, zlata ili sredstava koje je ostavila korumpirana vlada ili njen službenik i ako pristanete da primite ta sredstva na svoj račun, dobit ćete za uslugu veliki iznos kada se stvari smire. Kao i sve slične prijevare, reći će vam da najprije morate platiti poreze, bankovne pristojbe za anti-terorističke provjere i provjere pranja novca prije nego što vam pošalju novac.

Ove prijevare obično dolaze iz inozemstva i od vas se traži plaćanje putem žičanog prijenosa, ali od vas mogu također tražiti i bankovne prijenose ili druge načine plaćanja.

Ako padnete na ove prijevare, od prevaranta nikada nećete dobiti ništa i izgubit ćete novac koji ste poslali.

Zaštitite se

- Zapamtite da ne postoje brze sheme bogaćenja: ako zvuči previše dobro da bi bilo istinito, vjerojatno i jeste.
- Izbjegnite bilo kakav dogovor sa strancem koji traži uplatu unaprijed putem bankovne uplatnice, žičanog prijenosa, prijenosa međunarodnih sredstava, učitane kartice ili elektroničke valute. Rijetko je moguće povratiti novac poslan na ovaj način.
- Ako vam nepoželjni email izgleda sumnjivo, izbrišite ga. Nemojte kliknuti na poveznice.
- Vladini odjeli, banke ili komunalne tvrtke nikada vas neće kontaktirati tražeći da unaprijed uplatite novac kako biste potraživali pristojbu ili rabat.
- Ako niste sigurni, neovisno provjerite identitet kontakta. Ne koristite podatke navedene u poruci koja vam je poslana - nađite točne podatke o kontaktu putem neovisnog izvora, kao što je telefonski imenik ili pretraživanje preko interneta.
- Provedite internet-pretragu koristeći točne fraze koje se nalaze u ponudi – puno prijevara je identificirano na taj način.

Prijevare putem nagrada i lutrija

Nemojte da vas se nasamari iznenadnim dobitkom — nagradu dobivaju samo prevaranti.

Kako ovakve prijevare uspijevaju

Ovim prijevarama pokušava vas se nagovoriti da unaprijed uplatite novac ili date osobne podatke kako biste podigli dobitak od lutrije, nagradne igre ili natjecanja u koje nikada niste ušli. Prevaranti će tvrditi da morate platiti pristojbe ili poreze prije nego što vam se vaš „dobitak“ ili nagrada mogu predati. Možda ćete također morati nazvati ili poslati tekst na telefonski broj koji naplaćuje visoku stopu za korištenje kako biste primili nagradu. Tzv.

scratchie prijevare uključuju dobivanje pošiljke koja sadrži blještave brošure i nekoliko scratchie kartica, od kojih će jedna biti dobitna. Da bi sve bilo uvjerljivije, često će to biti druga ili treća nagrada. Kada ih nazovete da biste potraživali svoju nagradu, prevaranti će zatražiti plaćanje pristojbi ili poreza prije nego što je možete dobiti.

Lotto prijevare mogu koristiti nazive pravih inozemnih lutrija kako bi tvrdili da ste osvojili novac, iako nikada niste ušli u njih. Prevaranti obično mogu tražiti pristojbe ili naplatu poreza za oslobađanje sredstava. Također će vam reći da trebaju vaše osobne podatke kako bi dokazali da ste pravi dobitnik, ali zatim upotrijebiti ove informacije da bi vam ukrali identitet ili novac s bankovnog računa.

Lažni vaučeri i poklon kartice uključuju prijevare kroz koje dobivate e-mail, tekst ili poruku s društvenih medija u kojoj se tvrdi da ste osvojili poklon-karticu za šoping u poznatoj trgovini, ali trebate navesti neke detalje prije nego što je možete zatražiti. To je pokušaj da se dobiju osobne informacije koje se mogu koristiti za krađu identiteta ili da vas se cilja s nekom drugom prijevarom. Takve ponude poznate su kao isporuka ransomwarea na vašem računalu (pogledajte stranicu 17).

Kod **nagradnih igara za osvajanje putovanja** prevaranti tvrde da ste osvojili besplatan odmor ili avionske karte. Ono što ste zapravo osvojili je prilika za kupnju vaučera za smještaj ili let. Ovi putni vaučeri često imaju skrivene pristojbe i uvjete, ili mogu biti lažni i bezvrijedni. Isto tako, prevaranti vam mogu ponuditi nevjerojatne pakete s popustom koji jednostavno ne postoje.

Zaštitite se

- Zapamtite: ne možete osvojiti novac kroz nagradnu igru ili natjecanje ukoliko u njima niste sudjelovali.
- Natjecanja i lutrije od vas ne traže da platite pristojbu kako biste mogli podići svoju nagradu—provedite pretragu preko interneta koristeći iste riječi i fraze koje se nalaze u ponudi. To će možda potvrditi da se radi o prijevari.
- Uvijek dobro razmislite prije no što nazovete ili tekstirate na broj koji počinje sa '19'—oni naplaćuju po izrazito visokim stopama.

Prijevare kroz internet-kupovinu, oglase i aukcije

Prevaranti vole lakoću kupovine preko interneta.

Kako ovakve prijevare uspijevaju

Korisnici i biznisi sve više kupuju i prodaju preko interneta. Nažalost, prevaranti vole "kupovati" žrtve preko interneta.

Prevaranti mogu napraviti vrlo uvjerljivu **lažnu internet stranicu prodajnog mjesta** koja izgleda kao da je prava, uključujući i društvene mreže poput Facebooka.Najočitiji znak da je internet stranica lažna je metoda naplate – budite oprezni ako se od vas traži da platite preko žičanog prijenosa ili drugih neuobičajenih metoda.

Prijevare koje uključuju internet aukcije uvjeravaju vas da imate još jednu priliku kupiti nešto na što ste prethodno stavili ponudu, jer je osoba koja je dobila aukciju odustala. Prevarant će od vas tražiti da platite izvan aukcijske internet stranice gdje je plaćanje sigurno; ako to učinite, vaš novac će biti izgubljen jer nećete dobiti ono što ste platili, a aukcijska internet-stranica neće vam moći pomoći.

Prijevare korištenjem internet-oglasa su uobičajene prijevare koje su usmjerene i prema kupcima i prema prodavačima. Kupci bi trebali biti na oprezu od prevaranata koji stavljaju lažne oglase na legitimnim internet-lokacijama za oglase. Oglasi mogu biti za bilo što - od najma nekretnina do kućnih ljubimaca, rabljenih automobila ili foto-

aparata, a često će biti jeftiniji. Ako pokažete zanimanje za predmet, prevarant može tvrditi da putuje ili se seli u inozemstvo, te da će vam njegov agent isporučiti robu nakon primitka uplate. Nakon uplate nećete primiti robu niti ćete moći kontaktirati prodavača.

Kad se radi o prodavačima, klasificirani prevarant će odgovoriti na vaš oglas s velikodušnom ponudom. Ako je prihvatite, prevarant će platiti čekom ili uplatnicom. Međutim, iznos koji primite je veći od dogovorene cijene. U ovom **preplaćenom** iznosu, "kupac" vam može reći da je to bila pogreška i da će od vas tražiti da nadoknadite višak iznosa prijenosom novca. Prevarant će se nadati da ćete prenijeti novac prije nego što otkrijete da je njihov ček odskočio ili da je novčanica bila lažna. Izgubit ćete novac, kao i robu koju ste prodali, ako ste je već poslali.

Zaštitite se

- Pronađite s kime zaista imate posla. Ako se radi o australskom prodavaču ili prodajnom mjestu, u puno ste boljoj poziciji da ispravite problem ukoliko se nešto desi.
- Provjerite da li je prodavač renomiran, osigurava li povrat novca i pruža li usluge rješavanja primjedbi.
- Izbjegavajte aranžmane koji zahtijevaju plaćanje unaprijed putem novčane uplatnice, žičanog prijenosa, prijenosa međunarodnih sredstava, unaprijed učitane kartice ili elektroničke valute. Rijetko se može povratiti novac poslan na ovaj način. Nikada nemojte slati novac niti davati podatke o svojoj kreditnoj kartici ili internet računu nikome koga ne poznajete ili kome ne vjerujete, a pogotovo nikad e-mailom.
- Plaćajte jedino preko sigurne opcije za plaćanje koja se nalazi na validnoj internet stranici —potražite internet stranicu čija adresa počinje sa 'https' ii ma simbol zaključanog lokota.
- Nikada nemojte prihvaćati ček ili novčani nalog na veću sumu od one za koju ste se dogovorili prilikom prodaje, ili unaprijed slati novac.

Prijevare usmjerene na kompjutere i mobilne uređaje

Zapamtite: sve što se može priključiti na internet je ranjivo.

Kako ovakve prijevare uspijevaju

Prevaranti s daljinskim pristupom zovu vas na telefon tvrdeći da je vaše računalo zaraženo virusima. Ako slijedite njihove upute omogućit ćete im pristup i kontrolu nad vašim računalom na kojem mogu ukrasti informacije ili instalirati zlonamjerni softver. Također vas mogu pokušati uvjeriti da kupite "antivirusni" softver, za koji se obično ispostavi da je preskup ili besplatno dostupan na internetu.

Zlonamjerni softver je izraz za sve zlonamjerne programe koji se mogu instalirati na vaše računalo ili druge uređaje - uključujući viruse, špijunski softver, ransomware, trojanske konje i zapisivače pritisaka tipki.

Zapisivači pritisaka tipki i špijunski softver omogućuju prevarantima da snimaju točno ono što tipkate na tipkovnici kako bi saznali lozinke i bankovne podatke ili pristupili osobnim podacima i poslali ih kamo žele. Jednom kada su ovi softveri instalirani, prevaranti mogu kontrolirati vaš e-mail i društvene medije te ukrasti sve podatke na

vašem uređaju, uključujući i lozinke. Oni također mogu koristiti vaš internet za slanje drugih shema prijevara vašim prijateljima i obitelji.

Ransomware je još jedna vrsta zlonamjernog softvera koji šifrira ili zaključava vaš uređaj kako biste bili spriječeni da ga koristite dok ne platite za njegovo otključavanje. Plaćanje ne znači da će vaš uređaj biti otključan ili bez skrivenih virusa, koji se također mogu širiti i zaraziti druga računala ili uređaje na vašoj mreži.

Malware se obično isporučuje putem e-maila i može se činiti da dolazi iz legitimnih izvora, kao što je npr. vaš pružatelj komunalnih usluga, vladina agencija ili čak policija koja tvrdi da vam izdaje novčanu kaznu. Nemojte kliknuti na poveznice ili otvarati privitke ako u njih niste potpuno sigurni. Tako možda preuzimate zlonamjerni softver. Ove prevare ciljaju i pojedince i tvrtke.

Zaštitite se

- Budite oprezni pri besplatnim preuzimanjima koja nude glazbu, igre, filmove i pristup internet-stranicama za odrasle. Tako vam se mogu instalirati štetni programi bez vašeg znanja.
- Osigurajte svoje uredske mreže, računala i mobilne uređaje. Ažurirajte sigurnosni softver, mijenjajte lozinke i redovito kopirajte (back up) podatke. Spremite sigurnosne kopije izvan radnog mjesta i izvan interneta.
- www.staysmartonline.gov.au objašnjava kako pravilno sigurnosno kopirati podatke i osigurati mobilne uređaje.
- Ne otvarajte privitke i nemojte otvarati poveznice u email-porukama ili društvenim medijima koje ste primili od nepoznatih osoba - samo pritisnite ‘Delete’.

Krađa identiteta

Sve prijevare imaju potencijal i za krađu identiteta. Zaštita od prijevara istodobno znači i osiguravanje vaših osobnih podataka.

Krađa identiteta je potemcijalna opasnost kod svake prijevare

Većina ljudi povezuje prijevare s pokušajima da vam se ukrade novac. Međutim, i vaši su podaci vrijedni za prevarante. Prevaranti kradu vaše osobne podatke da bi provodili kriminalne aktivnosti kao što su neovlaštene kupnje vašom kreditnom karticom ili korištenje vašeg identiteta za otvaranje bankovnih ili telefonskih računa. Oni mogu uzimati zajmove ili obavljati druge ilegalne poslove pod vašim imenom. Oni čak mogu prodati vaše podatke drugim prevarantima za daljnju ilegalnu uporabu.

Krađa identiteta može biti financijski i emocionalno razorna. Vraćanje identiteta može potrajati mjesecima, a štetne konsekvence takve krađe mogu trajati godinama.

Krađa osobnih podataka – prevaranti vas kontaktiraju iz vedra neba putem e-maila, telefona, Facebooka ili SMS-a pretvarajući se da su iz legitimne tvrtke, poput banke ili pružatelja telefonskih ili internetskih usluga. Usmjeravaju vas na internet stranicu tvrtke koja traži vaše osobne podatke za provjeru korisničkih zapisa zbog navodne tehničke pogreške. Ili se mogu pretvarati da su prodavači luksuznih proizvoda tvrdeći da netko pokušava koristiti vašu kreditnu karticu. Savjetuju vam da kontaktirate svoju banku, ali oni ne prekidaju vezu i drže otvorenu liniju. Kada pokušate nazvati banku, još uvijek razgovarate s prevarantima koji simuliraju pravi poziv, oponašaju osoblje banke

i traže vaš račun i sigurnosne podatke. U oba slučaja, prevaranti snimaju sve informacije koje im date i zatim ih koriste za pristup vašim računima.

Lažne ankete – Prevaranti nude nagrade ili poklone kao što su poklon-kartice za kupovinu u poznatim trgovinama u zamjenu za popunjavanje ankete preko interneta. Anketa zahtijeva da odgovorite na niz pitanja, uključujući i otkrivanje važnih identifikacijskih ili bankovnih podataka.

Kao dio bilo koje prijevare – prevaranti često traže osobne podatke i u drugim oblicima prijevara. U prijevari na lutriji, često traže vašu vozačku dozvolu ili putovnicu kako biste 'dokazali svoj identitet prije nego što vam oslobode nagradni fond'. U prijevarama vezanim za stranice za upoznavanje i romantične veze, oni mogu zatražiti informacije "radi sponzoriranja svoje molbe za vizu, kako bi vas posjetili u Australiji".

Zapamtite: Davanje osobnih podataka prevarantu može biti jednako opasno kao i davanje novca. Nemojte davati svoje osobne podatke i čuvajte ih na sigurnom.

Zaštitite se

- **Dobro razmislite što govorite i radite na internetu.**
  Budite oprezni pri davanju informacija o sebi na internetu, uključujući i društvene medije, blogove i druge internet forume. Zastanite i razmislite prije nego što popunite ankete, uđete u natjecanja, kliknete na poveznice ili privitke, ili čak na 'prijateljstvo', 'liking' ili 'sharing' nešto na internetu.
- **Čuvajte se bilo kakvog zahtjeva za vašim podacima ili novcem**
  Prevaranti će vas pokušati nasamariti da im date svoje podatke, prisvajajući i koristeći imena poznatih tvrtki ili vladinih odjela. Ako sumnjate da je nešto prijevara, ne odgovarajte. Pregledajte telefonski imenik ili napravite pretragu preko interneta da biste provjerili kontakt-pojedinosti dotične organizacije. Nikada nemojte koristiti kontakt -pojedinosti navedene u izvornom zahtjevu.

Ako ste prevarantima dali osobne identifikacijske podatke, kontaktirajte IDCARE na 1300 432 273.

Prijevare u svezi posla i zapošljavanja

Velika zarada—garantirano?
Malo sutra!

Kako ovakve prijevare uspijevaju

Prijevare u svezi posla i zapošljavanja uključuju ponude za rad od kuće ili za postavljanje i ulaganje u „poslovnu priliku“. Prevaranti obećavaju posao, visoku plaću ili veliki povrat ulaganja nakon početnih uplata unaprijed. Ove uplate mogu biti za “poslovni plan”, tečaj obuke, softver, uniforme, sigurnosne provjere, poreze ili pristojbe. Ako plaćate pristojbu, možda nećete primiti ništa ili pak ne ono što ste očekivali ili što su vam obećali.

Neke poslovne ponude mogu biti obmana da bi se prikrilo **protuzakonito pranje novca**, gdje se od vas traži da pozirate kao „voditelj računa“ ili „osobni asistent“, da za proviziju primate uplate na svoj bankovni račun, a zatim novac proslijedite inozemnoj tvrtki.

Ovakve prijevare se često promoviraju putem spam e-mailova ili reklamama u dobro poznatim oglasima i na internet-stranicama za traženje posla, pa čak i na vladinim internet stranicama za traženje posla.

Velika opasnost u svezi s ovim prijevarama je da se od vas može zatražiti puno osobnih podataka koje ne biste smjeli davati, uključujući i vaš porezni broj ili preslike putovnice ili vozačke dozvole. Te se informacije kasnije mogu koristiti za krađu identiteta.

Zaštitite se

- Čuvajte se ponuda ili programa koji tvrde da jamče dohodak ili koji traže plaćanje unaprijed.
- Nikada nemojte pristajati prenositi novac u nečije ime—to je pranje novca i protuzakonito je.
- Nemojte davati svoj porezni broj, vozačku dozvolu ili putovnicu kada se prijavljujete za posao. Možda ćete morati dati te informacije, ali tek nakon što počnete raditi.

Pranje novca je kazneno djelo: nemojte pristati prebacivati novac za nepoznatu osobu.

Dobrotvorne i medicinske prijevare

Prevaranti su bezdušni i mogu 'napasti' i tijekom razdoblja očajničke potrebe.

Kako ovakve prijevare uspijevaju

Prevaranti iskorištavaju osobe koje žele dati dobrovoljni prilog za dobrotvorne svrhe ili pronalaženje lijeka za zdravstveni problem.

U **dobrotvorne prijevare** uključeni su prevaranti koji prikupljaju novac pretvarajući se da rade za opravdane ili dobrotvorne svrhe ili za svrhu koju su sami izmislili. Oni će često iskoristiti i nedavnu prirodnu katastrofu ili krizu koja je bila u vijestima.

Ovakve prijevare odvraćaju ljude od prijeko potrebnih donacija legitimnim dobrotvornim organizacijama. Dobrotvorne organizacije moraju biti registrirane od strane vlade – najprije provjerite njihovu registraciju i zatim donirajte s pouzdanjem.

Čudotvorni lijekovi – prijevare koje nude niz proizvoda i usluga koji se mogu činiti zakonitim alternativnim lijekovima koji obično obećavaju brzo i učinkovito liječenje ozbiljnih zdravstvenih stanja. Liječenje se često reklamira lažnim svjedočenjima ljudi koji su 'izliječeni'.

Prijevare koje obećavaju dramatično mršavljenje s malo ili bez ikakvog napora. Ova vrsta prijevare može uključivati neuobičajenu ili restriktivnu dijetu, revolucionarnu vježbu, uređaj za razbijanje masti, najnovije pilule, flastere ili kreme. Od vas se može tražiti da uplatite veliki iznos unaprijed ili sklopite dugoročni ugovor kako biste mogli stalno primati proizvod.

Lažne internet ljekarne nude krivotvorene lijekove i lijekove po vrlo povoljnim cijenama, a ponekad ih nude i bez liječničkog recepta. Ovi lijekovi mogu imati ograničene ili nepostojeće aktivne sastojke, što može imati smrtonosne posljedice za korisnike.

Zaštitite se

- Ako vam je prišao ulični sakupljač priloga, zatražite njegovu identifikaciju. Ako imate ikakvih sumnji da osoba nije ono za što se izdaje, nemojte joj davati novac.
- Provjerite popis registriranih australskih dobrotvornih neprofitnih organizacija.
- Posavjetujte se sa svojim liječnikom ako razmišljate o korištenju "čudotvornih lijekova" ili "momentalnih rezultata", bilo da se radi o lijekovima, nadomjescima ili drugim oblicima tretmana.
- Zapitajte se: ako je ovo doista čudotvorni lijek, zar vam ga vaš zdravstveni djelatnik već ne bi spomenuo?

Poslovne prijevare

Prevaranti se okorištavaju prirodom brzog rada velikog broja današnjih biznisa, da bi ih prevarili.

Kako ovakve prijevare uspijevaju

Prijevare usmjerene ka tvrtkama pojavljuju se u raznim oblicima i vjerojatno će biti najfrekventnije u najhektičnijim razdobljima poslovanja, poput kraja financijske godine.

Lažna naplata najčešći je prijevarni trik usmjeren protiv poduzeća. Prevaranti izdaju lažne račune za neželjene ili neovlaštene objave, oglase, proizvode ili usluge. **Prijevara koja uključuje poslovni imenik je dobro poznati primjer,** gdje dobivate račun za uvrštenje u navodno dobro poznati telefonski imenik. Prevaranti će vas pokušati izigrati da se prijavite tako što će prikriti ponudu kao neplaćeni račun ili besplatni popis, ali sa skrivenim ugovorom o pretplati u sitnom tisku.

Prijevara koja uključuje ime domene je još jedan trik koji prevaranti koriste, gdje ste prevareni da se prijavite za neželjenu registraciju internetske domene vrlo slične vašoj. Također možete primiti i lažnu obavijest o obnavljanju stvarnog naziva vaše domene i platiti je da niste toga niti svjesni.

Prijevara glede uredske opskrbe uključuje primanje i naplatu proizvoda koje niste naručili. Ove prijevare često uključuju proizvode ili usluge koje redovito naručujete, poput pribora za pisanje i

potrošnog materijala za čišćenje. Prevaranti vas obično nazivaju pretvarajući se da je vaša usluga ili proizvod već naručen.

Prijevare s preusmjeravanjem plaćanja koriste se informacijama koje su dobili hakiranjem vaših računalnih sustava. Prevaranti zatim poziraju kao jedan od vaših redovitih dobavljača i kažu vam da su se njihovi bankovni podaci promijenili. Mogu vam reći da su nedavno promijenili banku i mogu koristiti kopije zaglavlja i zaštitne marke kako bi vas uvjerili da su legitimni. Oni će vam dati novi broj bankovnog računa i zatražiti da se sve buduće isplate procesiraju u skladu s novim informacijama. Takva prijevara se često otkriva samo onda kada vaš redoviti dobavljač upita zašto vaše narudžbe nisu plaćene.

Ransomware može biti vrlo štetan za bilo koji biznis. Najbolja obrana je redovito sigurnosno kopiranje podataka i pohranjivanje sigurnosnih kopija izvan istog mjesta i izvan internet mreže. Više informacija na stranici 17.

Zaštitite se

- Nemojte odmah pristati na ponude ili dogovore - uvijek zatražite pisanu ponudu i potražite neovisni savjet ako posao uključuje novac, vrijeme ili dugoročnu obvezu.
- Nikada ne pružajte bankovne, financijske i računovodstvene podatke svoje tvrtke nekome tko vas neočekivano kontaktira ili koga ne poznajete i kome ne vjerujete.
- Učinkoviti postupci radnog poslovanja mogu znatno pridonijeti sprečavanju prijevara – oni imaju jasno definirane postupke za provjeru i plaćanje računa i faktura te vrlo pažljivo provjeravaju zahtjeve za promjenu bankovnih podataka.
- Educirajte svoje osoblje da prepozna prijevare.
- Kopirajte svoje poslovne podatke i pohranite ih izvan radnog mjesta i izvan interneta.
- Čuvajte se e-maila koji od vas traže izmjene pojedinosti o plaćanju. Uvijek takve zahtjeve provjerite izravno kod tvrtke ili relevantnog pojedinca.

Kako prijevare funkcioniraju—anatomija prijevare

Većina prijevara koristi se istom shemom i jednom kada je budete razumjeli, trikove će biti jednostavnije prepoznati.

Ako pažljivo pogledate sve vrste prijevara navedene u ovoj knjižici, uskoro ćete primijetiti da većina prijevara prolazi kroz tri faze: (1) pristup; (2) komunikacija; i (3) plaćanje.

Razumijevanje osnovnih faza takvih prijevara pomoći će vam da izbjegnete trenutnu bujicu prijevara i budete na oprezu od novih prijevara koje će se pojaviti u budućnosti.

1. Pristup: metoda dostave

Kada vam prevaranti pristupe, uvijek će imati priču koja je dizajnirana da u nju povjerujete. Prevaranti se uvijek pretvaraju da su nešto što nisu: npr. vladin djelatnik, stručni investitor, lutrijski službenik ili čak i romantični obožavatelj.

Da bi vam dostavili ove laži, prevaranti će se služiti raznim metodama komunikacije.

Preko interneta

Prevaranti vrebaju iza anonimnog okoliša interneta.

E-mail je omiljena metoda dostave prijevara, jer pruža jeftin i jednostavan način komunikacije na velikoj skali. E-maili kojima se "pecaju" vaši osobni podaci, najčešći su oblici prijevare korištenjem e-maila.

Platforme za društveno umrežavanje, internet stranice za upoznavanje i internetski forumi omogućuju prevarantima da se "sprijatelje" s vama i da uđu u vaš osobni život kako bi pristupili vašim osobnim podacima, koji se zatim mogu koristiti protiv vas ili vaše obitelji i prijatelja.

Kupovina preko interneta, oglasi i aukcijske internet-stranice prevaranti koriste da bi došli do kupaca i prodavača, pri čemu se početni kontakt često odvija putem poznatih i pouzdanih ili pak lažnih internet stranica koje izgledaju kao prava stvar. Potražite sigurne opcije plaćanja i čuvajte se neobičnih načina plaćanja kao što su žičani transfer, Bitcoins ili unaprijed učitane novčane kartice. Kreditne kartice obično nude neku zaštitu.

Preko telefona

Prevaranti također zovu preko telefona i šalju tekst poruke

Veliki je broj prijevara - uključujući i prijeteće pozive glede povrata poreza, pa sve do ponuda nagrada ili „pomoći“ s računalnim virusima. Dostupnost jeftinih VOIP telefonskih protokola znači da pozivni centri mogu operirati iz inozemstva, s telefonskim brojevima koji izgledaju kao mjesni brojevi. Identifikacija telefonskog pozivatelja može se lako prikriti i jedan je od mnogih trikova koje prevaranti koriste kako bi vas uvjerili da su oni netko drugi.

SMS poruke prevaranti koriste za slanje cijelog niza shema, uključujući razna natjecanja ili prijevare koje uključuju prijevare o nagradama. Ako odgovorite, možda će vam se naplaćivati visoke telefonske pozivne stope ili ćete se možda nehtijući prijaviti za uslugu pretplate. Sigurnije je ne odgovarati i ne otvarati poveznice u tekstualnim porukama, osim ako znate od koga su došle. One mogu sadržavati i privitke ili poveznice sa zlonamjernim softverima u obliku fotografija, pjesama, igara ili aplikacija.

Na vašim vratima

Pripazite se—neki prevaranti vam se mogu pojaviti na vratima.

Prijevara od vrata do vrata obično uključuje prevaranta koji promovira proizvode ili usluge koje nisu isporučene ili su vrlo loše kvalitete. Može vam se čak i naplaćivati za posao koji niste željeli ili na što niste pristali. Uobičajene prijevare od vrata do vrata provode nepošteni poduzetnici koji se kreću od mjesta do mjesta i rade kućne popravke ili jednostavno uzimaju novac i bježe.

I legitimni poduzetnici mogu prodavati od vrata do vrata, ali moraju jasno identificirati sebe i svoju tvrtku i slijediti ostala pravila. Vi imate određena prava kada je riječ o prodajnim praksama od vrata do vrata, uključujući i mogućnost da se predomislite - saznajte više na www.accc.gov.au/doortodoor.

Prevaranti se mogu predstavljati kao **lažni dobrotvorni radnici za prikupljanje donacija.** Iskoristit će nedavne kataklizme poput poplava i požara. Prije davanja donacije zatražite identifikaciju i pogledajte njihovu službenu knjigu računa.

Grupno slanje e-maila se još uvijek koristi za slanje lažnih **lutrija i nagradnih igara, mogućnosti ulaganja, nigerijskih prijevara i lažnih pisama o nasljeđu.** Blještava brošura nije jamstvo da je ponuda legitimna.

Bez obzira na način dostave, njihova priča je uvijek mamac i ako zagrizete, prevarant će vas pokušati gurnuti u sljedeću fazu.

2. Komunikacija i priprema

Ako im date priliku da vam se obrate, počet će koristiti trikove iz svoje **zalihe prijevara** kako bi vas nagovorili da se oprostite od svog novca.

Prevarantski trikovi uključuju slijedeće:

- Daju vam razrađene, ali **uvjerljive priče** da bi dobili ono što žele.
- Koriste vaše **osobne podatke** kako bi vas uvjerili da ste se s njima već ranije susreli, da bi prijevaru prikazali legitimnim poslom.
- Prevaranti vas mogu **redovito kontaktirati** kako bi izgradili povjerenje, uvjerili vas da su vaš prijatelj, partner ili romantično zainteresirani.
- **Igraju se s vašim emocijama** koristeći uzbuđenje koje donosi pobjeda, obećanje vječne ljubavi, sućut prilikom tragedije, osjećaj krivnje zbog nedavanja pomoći ili pak osjećaj tjeskobe i straha od uhićenja ili kazne.
- Prevaranti vole stvoriti **osjećaj hitnosti** kako ne biste imali vremena razmišljati o stvarima i kako biste reagirali na emocije, a ne koristili logiku.
- Slično tome, oni koriste **prodajnu taktiku pod visokim pritiskom** govoreći da je nešto ograničena ponuda, da će cijene rasti ili da će se tržište promijeniti i ta mogućnost će biti izgubljena.
- Prijevara može imati sva obilježja stvarnog poslovanja korištenjem blještavih brošura s tehničkim žargonom industrije koje su poduprte fasadom ureda, pozivnim centrima i profesionalnim internet-stranicama.
- S pristupom internetu i pametnom softveru prevarantima je lako stvoriti krivotvorene i službene dokumente. Dokument koji izgleda kao da ima vladino odobrenje ili je ispunjen pravnim jezikom može prevarantima dati osjećaj autoriteta.

Sheme prevaranta su osmišljene kako bi vas privolili da se otvorite, povjerujete u njihovu priču i reagirate brzo ili iracionalno - i nastavite vjerovati do završne faze, tj. do slanja novca.

3. Slanje novca

Ponekad je način na koji će prevarant tražiti od vas da izvršite uplatu najbolji način da otkrijete prijevaru.

S potraživanjem novca može se započeti nakon nekoliko minuta od primarnog kontakta ili pak nakon nekoliko mjeseci brižljivog kondicioniranja. Prevaranti imaju svoje omiljene načine kako žele da im pošaljete novac.

Poznato je da prevaranti usmjeravaju žrtve na **najbliže mjesto** za slanje novca (npr. pošta, žičani prijenos ili čak banka). Poznato je da oni ostaju na telefonu, daju specifične upute i čak vam mogu poslati taksi kako bi vam pomogli. Prevaranti su spremni prihvatiti novac na bilo koji način i to može uključivati **izravne bankovne transfere, unaprijed učitane debitne kartice, poklon kartice, Google Play, Steam ili iTunes kartice ili virtualnu valutu kao što je Bitcoin**. Svaki zahtjev za plaćanje neuobičajenom metodom je znak da je to dio moguće prijevare.

Kreditne kartice obično nude neku zaštitu, ali trebali biste potražiti sigurne opcije plaćanja u kojima se na internet-adresi pojavljuje "https", a internet-lokacija ima zatvoreni simbol lokota.

Ne šaljite novac nekome koga znate samo preko interneta ili telefona - osobito ako je ta osoba u inozemstvu.

Budite svjesni da prevaranti također mogu tražiti i plaćanje u obliku vrijedne robe i skupih darova, kao što su nakit ili elektronika.Slanje novca prevarantima nije jedina stvar koja bi vas trebala zabrinjavati - ako nepoznatoj osobi pomognete prebaciti novac, možda ćete nesvjesno biti uključeni u nezakonite aktivnosti pranja novca.

Zlatna pravila kako ćete se zaštititi

Budite svjesni činjenice da prijevare postoje. Kada imate posla s nepoznatim kontaktima, bilo da se radi o ljudima ili tvrtkama, bilo telefonom, poštom, e-mailom, osobno ili na društvenoj mreži, uvijek budite svjesni mogućnosti da se možda radi o prijevari. Zapamtite, ako izgleda previše dobro da bi bilo istinito, vjerojatno to i jeste.

Znajte s kim imate posla. Ako ste se ikada upoznali s nekim preko interneta ili niste sigurni u legitimnost nekog biznisa, odvojite malo vremena i napravite malo više istraživanja. Napravite Google pretragu slika ili preko interneta potražite druge osobe koje su možda imale posla s njima.

Ne otvarajte sumnjive tekstove, pop-up prozorčiće ili e-mail poruke - izbrišite ih. Ako niste sigurni, provjerite identitet kontakta putem neovisnog izvora kao što je telefonski imenik ili internet-pretraživanje. Ne koristite kontakt podatke navedene u sumnjivoj poruci koja vam je poslana.

Osigurajte svoje osobne podatke. Stavite bravu na poštanski sandučić i uništite račune i druge važne dokumente prije nego što ih bacite. Držite vaše lozinke i pin-brojeve na sigurnom mjestu. Budite vrlo oprezni kada se radi o tome koliko osobnih podataka dajete na internet-stranicama društvenih medija. Prevaranti mogu koristiti vaše podatke i slike za stvaranje lažnih identiteta ili da vas pokušaju prevariti.

Čuvajte se neuobičajenih načina plaćanja. Prevaranti često traže plaćanje putem žičanih transfera, unaprijed učitane kartice, pa čak i Google Play, Steam ili iTunes kartice i Bitcoin-a. To je gotovo uvijek znak da je to dio prijevare.

Zaštitite svoje mobilne uređaje i računala. Uvijek koristite zaštitu lozinkom, ne dijelite pristup s drugima (uključujući i daljinski), ažurirajte sigurnosni softver i kopirajte sadržaj. Zaštitite svoju WiFi mrežu lozinkom i izbjegavajte korištenje javnih računala ili WiFi pristupnih točaka za pristup financijskim transakcijama preko interneta ili pružanju osobnih podataka.

Pažljivo odaberite svoje lozinke. Odaberite lozinke koje bi drugima bilo teško pogoditi i redovito ih mijenjajte. Jaka lozinka treba sadržavati kombinaciju velikih i malih slova, brojeva i simbola. Nemojte koristiti istu lozinku za svaki račun/profil i ne dajte svoju lozinku nikome.

Čuvajte se bilo kakvih zahtjeva za davanje svojih podataka i novca. Nikada nemojte slati novac niti davati brojeve kreditnih kartica, podatke o elektronskim računima ili kopije osobnih dokumenata nikome koga ne poznajete ili kome ne vjerujete. Nemojte pristati na prijenos novca ili robe za nekog drugog: pranje novca je kazneno djelo.

Budite oprezni prilikom kupovine preko interneta. Čuvajte se ponuda koja izgledaju previše dobro da bi bile istinite i uvijek koristite usluge internet-transakcija i kupovine koje znate i kojima vjerujete. Razmislite dvaput prije korištenja virtualnih valuta (kao što je Bitcoin) - one nemaju istu zaštitu kao druge transakcijske metode, što znači da novac ne možete dobiti natrag kada ga pošaljete.

Gdje potražiti pomoć i podršku

Ako ste prijevarom izgubili novac ili ste svoje osobne podatke dali prevarantu, malo je vjerojatno da ćete dobiti novac natrag. Međutim, postoje koraci koje možete poduzeti odmah kako biste ograničili štetu i zaštitili se od daljnjih gubitaka.

Kontaktirajte svoju banku ili kreditnu udrugu

Ako ste prevarantu poslali novac ili dali osobne bankovne podatke, odmah kontaktirajte svoju banku ili kreditnu udrugu. Možda ćete moći zaustaviti prijenos novca ili provjeriti ili zatvoriti račun, ako prevarant ima podatke o vašem računu. Izdavač kreditne kartice možda će vam moći izvršiti "povratnu naplatu" (obrnuti transakciju) ako je vaša kreditna kartica protuzakonito korištena.

Povratite ukradeni identitet

Ako sumnjate da ste žrtva krađe identiteta, važno je brzo reagirati kako biste smanjili rizik od financijskog gubitka ili druge štete.

Kontaktirajte **IDCARE** - besplatnu službu koju financira vlada i koja pruža podršku žrtvama krađe identiteta. IDCARE vam može pomoći da napravite plan sanacije štete kako biste poduzeli odgovarajuće korake za oporavak svog ugleda, kreditne povijesti i identiteta. Posjetite internet-stranicu IDCARE na adresi www.idcare.org ili nazovite 1300 432 273.

Podnesite zahtjev za **Commonwealth Victims' Certificate** – ovaj certifikat za žrtve na području Commonwealtha podržava vašu tvrdnju da ste bili žrtva krađe identiteta i može se upotrijebiti za ponovno uspostavljanje kredibiliteta kod vlade ili financijskih institucija. Posjetite Odjel državnog odvjetnika (Attorney-General's Department) na www.ag.gov.au (ili nazovite 02 6141 6666) kako biste saznali više o zaštiti i povratu svog identiteta.

Posjetite službu za savjetovanje ili podršku

Ako ste vi ili netko koga poznajete bili prevareni i možda patite od emocionalnog stresa ili depresije, obratite se svom liječniku opće prakse, mjesnom zdravstvenom djelatniku ili nekome kome vjerujete. Možete kontaktirati savjetodavne ili pomoćne službe, kao što su:

Lifeline - kada trebate podršku u krizi, kontaktirajte Lifeline na 13 1114 (24/7) ili posjetite www.lifeline.org.au

Beyondblue - za informacije o depresiji ili anksioznosti, kontaktirajte beyondblue na 1300 224 636 ili posjetite www.beyondblue.org.au

Telefonska linija za pomoć djeci (Kids helpline) - telefonska i internet savjetodavna služba za mlade osobe u dobi od pet do 25 godina. Obratite se službi za pomoć djeci na 1800 551 800 ili posjetite www.kidshelpline.com.au

Financijsko savjetovanje Australija (Financial Counselling Australia) - ako ste u financijskim teškoćama, nazovite 1800 007 007 kako biste razgovarali s besplatnim financijskim savjetnikom ili posjetite www.financialcounsellingaustralia.org.au.

Gdje prijaviti prijevaru

Prijavom prijevara odgovarajućim vlastima možete pomoći drugim osobama. Vaše informacije pomoći će tim organizacijama da dobiju bolju sliku o najnovijim prijevarama i upozore druge o tome na što obratiti pažnju.

Sljedeće organizacije primaju priopćenja o određenim vrstama prijevara.

Scamwatch

Prijavite prijevare ACCC-u preko Scamwatch-a —posjetite www.scamwatch.gov.au

Budite jedan korak ispred prevaranata

Budite jedan korak ispred prevaranata - posjetite internet stranicu organizacije Scamwatch kako biste dobili uvid u prijevare usmjerene ka australskim potrošačima i malim tvrtkama. Saznajte više o tome kako te prijevare funkcioniraju, kako se od njih zaštititi i saznajte što učiniti ako ste žrtva prijevare.

Registrirajte se za usluge Scamwatch-a kako biste primali besplatne obavijesti putem e-maila o najnovijim oblicima prijevara.

www.scamwatch.gov.au

Pratite Scamwatch preko Twittera na @scamwatch_gov ili http://twitter.com/Scamwatch_gov

Ako iskusite prijevaru na internet stranici ili platformi društvenih medija, prijavite je toj istoj stranici kako bi je oni mogli istražiti i ukloniti. Ako se prevaranti izdaju za legitimnu organizaciju poput vladinog odjela ili banke, obavijestite tu organizaciju kako bi ona mogla upozoriti druge korisnike.

Druge agencije

Trebali biste također možda prijaviti i prijevaru koju ste sami iskusili, agencijama koje se specifično bave ispitivanjem određenih vrsta prijevara.

Vrsta prijevare	Agencija
Cybercrime	Australska mreža za izvješćivanje o cyber kriminalu (Australian Cybercrime Online Reporting Network (ACORN))—visit www.acorn.gov.au
Financijske i investicijske prijevare	Australska sigurnosna komisija za investicije (Australian Securities and Investments Commission (ASIC))—posjetite www.moneysmart.gov.au ili nazovite ASIC infoliiju na 1300 300 630
Prijevara i krađa	Vaša mjesna policijska služba—nazovite 13 1444
Spam e-maili i SMS-i	Australsko tijelo za komunikacije i medije (Australian Communications and Media Authority (ACMA))—posjetite www.acma.gov.au ili nazovite ACMA korisnički centar na 1300 850 115
Prijevare vezane za povrat poreza	Australian Taxation Office (ATO) (Australski porezni ured (ATO)) – ako želite prijaviti prijevaru vezanu za povrat poreza ili provjeriti da li je osoba koja vas je kontaktirala iz ATO-a legitimna: • Nazovite 1800 008 540 ili proslijedite email o poreznoj muljaži koji vam je poslan na ReportEmailFraud@ato.gov.au
Financijska pitanja	Vaša banka ili financijska institucija

Kontaktirajte svoju mjesnu agenciju za zaštitu potrošača

Iako je ACCC nacionalna agencija koja se bavi općim pitanjima zaštite potrošača, državne i teritorijalne agencije mogu vam također pomoći.

Ured regulatornih službi Australskog glavnog grada (Australian Capital Territory Office of Regulatory Services)	www.accesscanberra.act.gov.au 13 2281
Consumer Affairs Victoria	www.consumer.vic.gov.au 1300 558 181
New South Wales Fair Trading	www.fairtrading.nsw.gov.au 13 3220
Northern Territory Consumer Affairs	www.consumeraffairs.nt.gov.au 1800 019 319
Queensland Office of Fair Trading	www.fairtrading.qld.gov.au 13 7468
Potrošačke i poslovne usluge u South Australia (South Australia Consumer and Business Services)	www.cbs.sa.gov.au/ 13 1882
Tasmanijske potrošačke, građevinske i profesionalne usluge (Tasmania Consumer, Building and Occupational Services)	www.cbos.tas.gov.au/ 1300 654 499
Odjel za rudarstvo, regulativu i sigurnost industrije u Western Australia (Western Australia Department of Mines, Industry Regulation and Safety)	www.consumerprotection.wa.gov.au/ 1300 304 054

Više informacija

Australska vlada preko interneta nudi neke od vrlo dobrih resursa koji će vam pomoći da ostanete zaštićeni na internetu.

- Stay Smart Online služba—www.staysmartonline.gov.au
- CyberSmart internet stranica—www.cybersmart.gov.au
- Stay Smart Online vodič—dostupan na www.staysmartonline.gov.au/get-involved/guides

www.scamwatch.gov.au