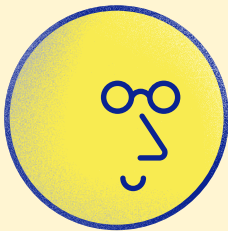


Paano malalaman at maiiwasan ang mga scam (panloloko)



Ang iyong gabay para
maprotektahan ang sarili
laban sa mga scam



Australian Government



National
Anti-Scam
Centre



ScamWatch
Stop. Better safe than scammed.

Pagkilala sa lupain

Kinikilala ng ACCC ang mga tradisyonal na may-ari at katiwala ng Lupain sa buong Australya at kinikilala ang kanilang patuloy na koneksyon sa lupa, dagat at komunidad. Nagbibigay-galang kami sa kanila at sa kanilang mga kultura; at sa kanilang mga Elder sa nagdaan, kasalukuyan at hinaharap.

Australian Competition and Consumer Commission
Ngunnawal

23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

© Komonwelt ng Australya 2023

Ang gawain na ito ay may copyright. Bukod sa anumang paggamit na pinahihintulutan sa ilalim ng *Copyright Act 1968*, lahat ng mga materyal na nakapaloob sa gawaing ito ay ibinigay alinsunod sa lisensya ng Creative Commons Attribution 4.0 Australia, maliban lamang sa:

- Commonwealth Coat of Arms
- mga logo ng ACCC at AER
- Ang anumang ilustrasyon, dayagram, litrato o graphic kung saan ang Australian Competition and Consumer Commission ay walang hawak na copyrighti, ngunit maaaring bahagi ng/o nakalagay sa lathalaing ito.

Ang mga detalye ng mga kaugnay na mga kundisyon ng lisensya ay makukuha sa website ng Creative Commons, pati na rin ang buong mga batas para sa lisensyang CC BY 4.0 AU.

Ang mga kahilingan at katanungan tungkol sa pagkopya at mga karapatan ay dapat na idaan sa Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

Mahalagang pahayag

Ang impormasyon sa lathalaing ito ay para sa pangkalahatang patnubay lamang. Hindi ito bumubuo ng legal o iba pang propesyonal na payo, at hindi dapat asahan bilang pahayag ng batas sa anumang hurisdiksyon. Dahil sinadya lamang ito bilang isang pangkalahatang patnubay, maaaring naglalaman nito ng mga pangkalahatang impormasyon. Dapat kang kumuha ng propesyonal na payo kung mayroon kang anumang partikular na pag-aalala.

Ginawa ng ACCC ang lahat ng makatwirang pagsisikap upang makapagbigay ng napapanahon at tumpak na impormasyon, ngunit ito ay hindi magbibigay ng anumang mga garantiya tungkol sa kawastuhan, pagiging napapanahon o pagkakumpleto ng impormasyong ito.

Ang mga partidong gustong muling ilathala o dili kaya'y gamitin ang impormasyon sa lathalaing ito ay dapat suriin muna ang impormasyong ito kung napapanahon at wasto bago ilathala. Ito ay dapat gawin bago ang bawat edisyon ng paglalathala, dahil palaging nagbabago ang pamamatuubay at kaugnay na transisyonal na batas ng ACCC. Ang anumang mga katanungan ng mga partido ay dapat ipadala sa Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 05/24_24-13

www.accc.gov.au

Mga Nilalaman

May makukuhang tulong kung kinakailangan	1
Ano ang isang scam	3
Mga simpleng hakbang upang makilala at maiwasan ang Mga scam	4
Mga scam na text o SMS	7
Mga scam na email	11
Mga scam sa telepono	15
Mga scam na website	19
Mga scam sa social media, mga nakabase sa app at online messaging	23
Mga pangunahing scam na dapat mong malaman	27
Saan dapat isumbong ang mga scam	31
Karagdagang tulong at suporta	33



Ang gabay na ito ay isinulat ng National Anti-Scam Centre (Pambansang Sentro Laban sa Scam) at matutulungan kang kilalanin at protektahan ang iyong sarili mula sa pinsalang dulot ng mga scam.

Ang scam ay isang krimen at ang mga taong gumagawa ng mga scam ay mga kriminal. Maraming mga tao sa Australya ang niloloko at nawawalan ng kanilang pera, minsan ay pati na rin ang kanilang mga inipon sa buhay. Ang mga scam ay nakakasakit sa buhay ng mga tao.

Ang mga scam ay mas nagiging mahirap matukoy, kaya't kailangan nating magtutulongan upang sugpuin ang mga ito.

Nagtatrabaho ang National Anti-Scam Centre upang panatilihin ligtas ang mga Australyano laban sa mga scam.

Nakikipagtulungan kami sa pamahalaan at industriya upang makahanap ng mga paraan upang pigilin ang mga scammer sa pagnanakaw ng pera at personal na impormasyon mula sa mga Australyano. Narito ang ilang mga paraan kung paano namin ginagawa ito.

Tinutulungan namin ang mga tao na makilala at maiwasan ang mga scam.

Sa pamamagitan ng Scamwatch ay nagbabahagi kami ng napapanahon na impormasyon tungkol sa mga scam at mga paraan kung paano mo mapoprotektahan ang iyong sarili laban sa mga scam.

Binubuwag namin ang mga scammer

Sa pamamagitan ng pangungulekta at pagbabahagi ng intelihensya sa buong pamahalaan at industriya, ginagawa naming mas mahirap para sa mga scammer na ipagpatuloy ang kanilang mga krimen at ginagawa naming mas madali para sa mga tao na makapagsumbong tungkol sa mga scam.



May makukuhang tulong kung kinakailangan

Kung binabasa mo ito, malamang na ikaw, o isang taong kilala mo ay na-scam. Sa kasamaang palad, hindi ka nag-iisa. Ang mga scam ay mas lalong nagiging sopistikado na nangunguhulugan na kahit sino ay maaaring ma-scam.

Kung na-scam ka na, mahalagang kumilos kaagad.

Kung nawalan ka ng pera sa isang scammer, makipag-ugnay sa iyong bangko o card provider.

Kontakin ang IDCARE sa [1800 595 160](tel:1800595160), www.idcare.org.

Nagtatagumpay ang mga scam dahil parang tunay ang mga ito. Ang mga scammer ay umaasa na hindi mo malalaman ang mga babala dahil nagmamadali ka, parang may magandang alok na hindi mo gustong makaligtaan, o dahil parang iyon ay mula sa isang taong pinagkakatiwalaan mo.

Protektahan ang iyong sarili mula sa mga scam sa pamamagitan ng pagsunod sa 3 hakbang na ito:

Huminto



Huwag magbigay ng pera o personal na impormasyon kaninuman kung hindi ka sigurado.

Ang mga scammer ay mag-aalok na tumulong sa iyo o hihilingan kang beripikahin ang iyong pagkakakilanlan. Magpapanggap silang galing sa mga organisasyon na kilala at pinagkakatiwalaan mo na kagaya ng mga provider ng serbisyo, pulisya, iyong bangko o mga serbisyo ng pamahalaan.

Suriin



Tanungin ang iyong sarili – hindi kaya peke ang mensahe o tawag?

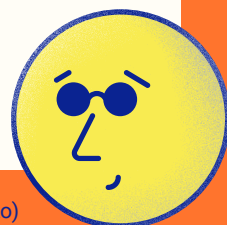
Huwag mo basta pindutin ang link sa isang message. Makipag-ugnay lamang sa mga negosyo o pamahalaan gamit ang impormasyon ng pakikipag-ugnay na mahahanap mo mula sa kanilang opisyal na website o app. Kung hindi ka sigurado, sabihin ang 'no', mag-hang up o i-delete.

Magsumbong



Kumilos kaagad kung may nararamdaman kang hindi tama.

Makipag-ugnay sa iyong bangko kung may mapansin kang hindi karaniwang aktibidad o kung nakuha ng isang scammer ang iyong pera o impormasyon. Magpatulong at isumbong ang scam sa ReportCyber at Scamwatch. Kapag isinumbong mo ang mga scam, tinutulungan mo ang lahat ng mga Australyano sa pagtatatag ng proteksyon laban sa mga scam.



Ano ang isang scam

Ang scam ay kapag nililinlang ka ng isang tao upang nakawin ang iyong pera o personal na impormasyon.

Ang mga scam ay mga krimen sa ekonomiya na isinasagawa ng mga kriminal na kadalasan ay napaka-organisado at sopistikado.

Ang mga scam:

-  ay isinasagawa ng mga kriminal
-  parang totoo
-  may kasamang mga kapani-paniwalang kwento
-  pinipilit kang gumawa ng aksyon

Ang scam ay HINDI:

-  Computer hacking
-  Mga hindi patas na tuntunin sa kontrata
-  Mga nanliligalig na pamamaraan ng pagbebenta

Mahalagang tandaan na hindi lahat ng mga negatibong karanasan ay mga scam. Maaaring may binayaran kang isang produkto na hindi mo natanggap o bumili ng isang bagay at natagpuan na ang kalidad nito ay hindi maganda. Habang ito ay nakakadismaya, ang mga ito ay maaaring hindi mga scam. Ang Australian Consumer Law ay nagbibigay ng mga proteksyon sa mga Australyanong mamimili para sa mga isyung katulad nito.

Para sa karagdagang impormasyon, bisitahin ang www.accc.gov.au/consumers

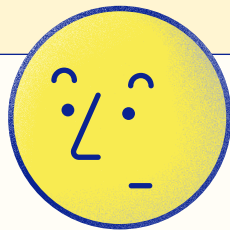
Mga simpleng hakbang upang makilala at maiwasan ang mga scam

Ang mga scam ay maaaring mangyari sa ating lahat. Gumagana ang mga scam dahil ang mga scammer ay lumilikha ng mga kapani-paniwalang kwento upang nakawin ang iyong pera at kunin ang iyong personal na impormasyon.

Nagiging matalino ang mga scammer at sinasamantala ang bagong teknolohiya, mga produkto, serbisyo, at mga pangunahing kaganapan upang kumbinsihin ka na ang kanilang mga scam ay totoo.

Maaaring napakahirap na malaman ang isang scam. Narito ang ilang mga sitwasyon na dapat pag-ingatan. Minsan ay gumagamit ang mga scammer ng kombinasyon ng mga taktikang ito.

- 1. Mga pagkakataon upang kumita o makatipid ng pera:**Lilinlangin ka ng mga scammer upang maniwala na makakakuha ka ng isang pambihirang benepisyo o alok. Pipilitin ka nilang agad kumilos upang hindi mo ito mapalampas. Tandaan, na ang mga transaksyong hindi kapani-paniwalang totoo ay kadalasang hindi totoo.
- 2. Mga malulungkot na kwento at paghingi ng tulong:**Susubukang samantalahin ng mga scammer ang iyong mabuting kalooban laban sa iyo. Ibabahagi nila sa iyo ang mga kwento ng kalungkutan at trahedya at ipapaliwanag kung bakit nila kailangan ang iyong tulong at pera.
- 3. Mga link at mga attachment:**Magpapadala ang mga scammer ng mga link upang papuntahin ka sa mga scam website na idinisenyo upang nakawin ang iyong impormasyon at pera. Maaari ring hilingin sa iyo ng mga scammer na buksan ang mga attachment. Makakapaglagay



ang mga ito ng mga virus na magnanakaw sa iyong impormasyon.

4. **Pipilitin kang kumilos kaagad:**Hindi gusto ng mga scammer na ikaw ay magpatumpik-tumpik at pag-isipan pa nang mabuti ang mga bagay-bagay. Pipilitin kang kumilos kaagad. Maaaring kabilang dito ang mga pagbabanta na may masamang mangyayari kung hindi ka kumilos kaagad.
5. **Hihilingin na magbayad ka sa hindi pangkaraniwan o partikular na mga paraan:**Kadalasan ay hihilingan ka ng mga scammer na magbayad gamit ang mga hindi pangkaraniwang pamamaraan katulad ng mga preloaded debit card, mga iTunes card, o virtual na pera katulad ng Bitcoin. Kapag nagastos na ang pera, hindi mo na ito mababawi pa.
6. **Mga kahilingang mag-set up ng mga bagong account o mga PayID:**Maaaring hilingan ka ng mga scammer na mag-set up ng isang bagong account sa bangko o PayID upang bayaran sila (o kaya'y mabayaran ka nila). Maaari silang magkunwari na sila ang iyong bangko at sasabihin sa iyo na ilipat ang iyong pera sa mga bagong account upang panatilihin itong ligtas.

Kung nagtagumpay ang mga scammer na makuha ang iyong pera, susubukan pa nilang kumuha ng karagdagang pera mula sa iyo. Sa kasamaang palad, isa sa bawat tatlong mga nabiktima ng scam ay na-scam na nang mahigit sa isang beses. Kung nawalan ka na ng pera sa isang scam, mag-ingat sa mga scammer na mag-aalok na tutulong sa iyo na maibalik ang iyong pera. Ito ay isa na namang uri ng follow-up scam.



Mga scam na text

o SMS

Ang mga scammer ay nagpapadala ng mga mensahe na nagpapanggap na mula sa pamahalaan, mga nagpapatupad ng batas, mga mapagkakatiwalaang negosyo, o pati na rin mula sa iyong kapamilya o mga kaibigan.

Ang mga mensaheng ito ay parang apurahan at eengganyuhin ka na kumilos kaagad. Kadalasan ay mayroon silang link na magdadala sa iyo sa isang scam website. Maaaring nakawin ng mga scammer ang anumang personal na impormasyon na i-enter sa mga scam website na ito at gagamitin upang kunin ang iyong pera o magsagawa ng panloloko sa pangalan mo.

Upang gawin na parang tunay ang mga mensaheng ito, kokopyahin o ikukubli ng mga scammer ang kanilang numero ng telepono sa likod ng numero ng telepono at caller ID ng mga lehitimong negosyo o mga taong kilala mo.

Maaari ring lumitaw ang mga scam na mensahe sa parehong message chain ng mga tunay na mensahe mula sa organisasyon, na ginagawa ang mga itong mas mahirap makilala.

Mga palatandaan na ang isang mensahe ay maaaring isang scam

Ang mensahe:



Hihilingan ka na magsagawa ng agarang aksyon, magsagawa ng isang pagbabayad, o maglipat ng pera.



Hihilingan ka na mag-click sa isang link o tumawag sa numero na ibinigay sa mensahe.



Hihilingan ka na mag-log on sa isang account sa online gamit ang iyong username at password o magbigay ng ibang karagdagang impormasyon.



Ay mula sa isang miyembro ng pamilya o kaibigan na nagsasabi na ang kanilang mga detalye ng pakikipag-ugnay ay nagbago.



Magbabanta na ihinto ang isang serbisyo o sisingilin ka kung hindi ka kikilos.



Magmumungkahi na ikaw o ang iyong mga account ay na-hack o kasangkot sa panloloko.



Magmumungkahi na may problema sa iyong bayad o sa paghahatid ng iyong pakete.

Mga hakbang upang protektahan ang iyong sarili laban sa mga scam na mensahe (messaging scams)



1. Kung ang isang kakilala mo ay magpapadala ng mensahe na nagsasabing may bago silang numero ng telepono:

- a. subukang tawagan siya sa kanilang dating numero na mayroon ka, at
- b. mag-mensahe sa kaniya sa bagong numero na may kasamang tanong na siya lamang ang makakasagot, upang masuri kung siya talaga ang sinasabing siya.



2. Huwag na huwag mag-click ng link sa mga mensahe.



3. Kung may link sa isang website ang isang mensahe, huwag pindutin ang link. Sa halip ay ikaw na mismo ang mag-search ng website sa online, o gamitin ang opisyal na app.



4. Huwag sagutin ang isang text message gamit ang numero ng telepono na ibinigay.



5. Magbalik-tawag sa organisasyon o tao sa numero ng telepono na sarili mong nahanap, tulad ng nagmula sa website ng organisasyon.



Mga scam na email

Ang mga scammer ay nagpapadala ng mga email na nagpapanggap na mula sa pamahalaan, mga nagpapatupad ng batas at mga negosyo. Ginagawa nilang parang apurahan upang kumilos ka kaagad.

Ginagamit ng mga scammer ang kaparehong logo at kaparehong email address ng tunay na organisasyon. Maaari ring kopyahin o itagoi ng mga scammer ang kanilang email address sa likod ng email address ng isang organisasyon o negosyo upang gawing mas parang tunay ang scam email.

Mga palatandaan na ang isang email ay maaaring isang scam

Ang email:



Humihiling ng bayad ngunit ang mga detalye ng account ay bago o nagbago mula sa iyong ginawang huling pagbabayad.



Hihilingan ka na mag-log on sa isang account sa online gamit ang iyong username at password o magbigay ng ibang karagdagang impormasyon.



Biglaan at kasama ang isang attachment na may imbitasyon na buksan ito.



Hihilingan ka na kumpirmahin ang iyong mga detalye sa bangko upang makatanggap ng isang refund o perang hindi mo inaasahan.



Ipapahayag na mayroong impormasyon tungkol sa iyo o mga larawan mo at nagbabanta na ilalabas ang mga ito.



Mag-aalok na tutulungan kang mabawi ang pera o kukuha ng bayad-pinsala para sa isang hindi awtorisadong pag-access ng datos (data breach) o paganakaw ng pagkakakilanlan.

Mga hakbang na maaari mong gawin upang protektahan ang iyong sarili mula sa mga email scam

1. Suriin na ang email ay tunay sa pamamagitan ng:



- a. direktang pakikipag-ugnay sa tao o organisasyon gamit ang mga detalye ng pagkontak na sarili mong hinanap tulad ng mula sa website ng organisasyon o,
 - b. pag-access sa organisasyon sa pamamagitan ng kanilang opisyal na app (hindi sa pamamagitan ng link).
-



2. Agad na ihinto ang pakikipag-ugnayan sa sinumang sinubukang magbanta o manakot sa iyo.
-



3. Huwag na huwag magbigay ng personal na mga detalye o bayaran ang sinumang nag-aalok sa iyo ng:
 - a. kompensasyon (bayad-pinsala) o tulong na makabawi mula sa isang nakaraang scam o hindi awtorisadong pag-access ng datos o,
 - b. mga gantimpala, mga premyo o isang pamana.
-



4. Gumamit ng multi-factor authentication (pagpapatunay) kung maaari. Ito ay nagbibigay ng karagdagang antas ng proteksyon at nangangahulugan na kailangan ng scammer ang email password at numero ng pin na ipinadala sa iyong telepono upang makapasok sa iyong email account.
-



Mga scam sa telepono

Tumatawag ang mga scammer, na nagsasabing mula sa mga kilalang organisasyon. Kabilang dito ang mga organisasyon ng pamahalaan, mga nagpapatupad ng batas, mga kumpanya ng pamumuhunan at batas, mga bangko, at mga provider ng telekomunikasyon.

Ginagawa nilang parang apurahan upang kaagad kang kumilos. Maaaring subukan nilang kumbinsihin ka na ibigay sa kanila ang iyong personal o mga detalye ng account mo sa bangko, o pag-access sa iyong computer.

Maaaring may ilang mga detalye na tungkol sa iyo ang tumatawag, tulad ng iyong pangalan o address, na ginagawang parang tunay ang tawag.

Mga palatandaan na ang isang tawag sa telepono ay maaaring isang scam

Ang tumatawag:



Humihingi ng kabayaran o humihiling sa iyo na magpadala ng pera sa isang bagong account.



Tatanungin ang iyong password, pin, one-time code, o ibang impormasyon ng seguridad.



Tatanungin ang iyong mga detalye ng pananalapi, tulad ng credit card o mga detalye ng bangko.



Hihilingan kang kumpletuhin ang isang gawain sa iyong teleponong mobile o computer na kagaya ng pag-install ng software o mag-access sa isang may seguridad na account.



Sasabihin na siya ay nagpapatupad ng batas (pulisya) at magbabanta sa iyo ng agarang pagkaaresto o deportasyon.



Sasabihin na ang iyong bangko o iba pang mga online na account ay na-hack o nasangkot sa panloloko.

Mga hakbang na maaari mong gawin upang protektahan ang iyong sarili mula sa mga scam sa telepono

1. Suriin na ang tawag ay tunay sa pamamagitan ng alinman sa dalawa:



- a. direktang pakikipag-ugnay sa tao o organisasyon gamit ang mga detalye ng pagkontak na sarili mong hinanap tulad ng mula sa website ng organisasyon o,
- b. pag-access sa organisasyon sa pamamagitan ng kanilang opisyal na app (hindi sa pamamagitan ng link).



2. Kung hindi ka sigurado kung sino ang tumatawag o kung nagbabanta o nananakot sa iyo, agad na mag-hang up.



3. Huwag kailanman mag-install ng software na pumapayag kaninuman na maka-access sa iyong computer o gadget.



4. Maaari mong hindi pansinin ang mga tawag mula sa mga numerong hindi mo alam o payagang mapunta ang mga tawag sa voicemail.



Mabuting malaman!

Maaari ka pa ring makakatanggap ng mga scam na tawag kahit magkakaroon ka ng pribadong numero o nasa Do Not Call register.



Mga scam na website

Maaaring magpanggap ang mga scammer na kahit sino sa online, pati na ang pamahalaan, isang tunay na negosyo, mga artista o iyong mga kaibigan o kapamilya.

Maaari silang lumikha ng mga pekeng website upang magmukha itong mga kilalang tatak. Maaari silang magpanggap na mga kilalang tao at gawing parang inaaprubahan nila ang mga paninda o serbisyo. Maaaring maglalaman ang mga website na ito ng mga pekeng review upang paniniwalaan mo sila.

Maaaring makita mo ang mga pekeng banner na patalastas o mga pop-up window na naglalaman ng mga pekeng babala o mga error message kapag nasa online.

Mga palatandaang maaaring scam ang isang website

Ang website:



Nag-aalok ng mga ibinebenta na masyadong napakamura kaysa karaniwan o kumpara sa ibang mga site.



Ibinabahagi sa iyo ang tungkol sa isang paraan upang kumita nang mabilis at madali na halos walang panganib o kahirap-hirap.



Naglalaman ng isang kagyat na babala o error message na hihiling sa iyo na pindutin ang isang link.



Hihingi ng bayad sa pamamagitan ng hindi karaniwan o partikular na mga paraan tulad ng mga gift card o cryptocurrency tulad ng Bitcoin.



Mga positibong review lamang ang naroon.

Mga hakbang na maaari mong gawin upang maiwasan ang mga scam sa website



1. Ikumpara ang mga presyo. Kung ang iniaalok ay mukhang hindi kapani-paniwala, malamang na ito ay hindi tunay.



2. Siyasatin ang organisasyon o taong kinakaharap mo bago mo ibigay ang iyong pera o personal na impormasyon.



3. Huwag magtiwala sa mga review na nakasulat mismo sa website na iyon. I-search ang website o pangalan ng negosyo at ang salitang 'scam' o 'reviews'.



4. Kung lilitaw ang isang babala (warning) o error message sa iyong screen, huwag itong pindutin, sa halip ay direktang magpunta sa aplikasyon na tinutukoy nito upang siyasatin kung ito ay tunay.



5. Panatiliing napapanahon ang gadget na ginagamit mo para sa online shopping sa pamamagitan ng pag-activate sa 'automatic updates' para sa iyong operating system at mga apps.



Mabuting malaman!

Ang mga praktikal na paraan upang maprotektahan ang iyong sarili sa online ay makukuha sa www.cyber.gov.au



Social media, app-based and online messaging scams

Kung may makikipag-ugnay sa iyo na hindi mo kilala sa social media, sa messaging platform tulad ng WhatsApp o WeChat, o sa pamamagitan ng isang app, maaaring ito ay isang scam.

Ang mga scammer na nagpapanggap na ibang tao ay kadalasang gumagamit ng tunay na litrato ng tao o opisyal na logo ng organisasyon na ipinapanggap nila, upang gawing mas mahirap na mahalata ang scam.

Ang mga scammer sa social media ay gagawa ng mga pekeng profile at magpapanggap na mula sa pamahalaan, isang tunay na negosyo, tagapag-employo, kumpanya ng pamumuhunan, o maging isang kaibigan, miyembro ng pamilya o minamahal.

Maaari silang magpanggap na mga sikat na tao at gawin na parang isinusulong nila ang mga paninda o serbisyo.

Maaari ring matutunan ng mga scammer ang napakamaraming bagay tungkol sa iyo mula sa mga detalye na ibinabahagi mo sa iyong mga account ng social media. Maaari nilang gamitin ang impormasyong ito upang hulaan ang iyong mga account password o targetin ka para sa ibang mga scam.

Mga palatandaan ng isang scam sa social media o app

Ang social media profile o app:



Ibinabahagi sa iyo ang tungkol sa isang paraan upang kumita nang mabilis at madali na halos walang panganib o kahirap-hirap.



limbitahan kang sumali sa isang kompetisyon o alok na may limitadong panahon.



Hihilingang ilipat ang pakikipag-usap mula sa isang app tulad ng dating app sa pribadong chat o email.



Imumungkahi na ang isang kilalang tao ay nag-eendorso o sumusuporta sa isang produkto o serbisyo.



Sasabihin na may bibili sa bagay na ibinebenta mo, kahit hindi pa nakikita at sa mataas na presyo.



Magbabantang ibahagi ang isang pribadong litrato mo, maliban kung babayaran mo sila ng pera.



Makikipag-ugnay sa iyo upang mag-alok ng trabaho.



Mabuting malaman!

Ang impormasyon kung paano mananatiling ligtas sa iba't-ibang mga plataporma ng social media ay matatagpuan sa www.esafety.gov.au

Mga hakbang na maaari mong gawin upang maiwasan ang mga scam sa social media at mga app-based scam



1. Siyasatin kung ang profile ay peke. Aktibo ba ang account? Gaano karami ang mga friend/follower nila at gaano karami ang mga post nila sa online?



2. I-search ang pangalan ng profile sa online kasama ang salitang 'scam.'



3. Huwag kailanman tumanggap ng trabaho na inialok sa iyo na walang pakikipanayam, o pag-uusap tungkol sa iyong karanasan, pagiging bagay, at mga reperensiya. Siyasatin ang recruiter at ang negosyo o indibidwal na nag-aalok ng posisyon. Makipag-ugnay sa recruitment agency sa pamamagitan ng mga numero ng telepono na mula sa sariling paghahanap sa internet. Huwag magbigay ng paunang bayad para makakuha lamang ng trabaho.



4. Kumuha lamang ng payo sa pamumuhunan mula sa taong lisensyado ng Australian Financial Services at tingnan kung ang isang kompanya o website ay hindi nakalista sa investor alerts portal ng International Organization of Securities Commission (IOSCO).



5. Huwag kailanman magbigay ng pera sa isang tao na nakilala mo lamang sa online. Madalas sabihin ng mga scammer na nakatira sila sa ibang bansa at hindi maaaring makita nang personal.



6. Huwag na huwag magpadala ng mga pribadong litrato ng iyong sarili sa sinumang nakilala mo lamang sa online.

Para sa karagdagang impormasyon tungkol sa mga scam, pati na ang ibang mga paraan ng pagkontak sa iyo ng mga scammer, halimbawa, sa personal at sa pamamagitan ng email, bisitahin ang [Scamwatch](#).



Mga pangunahing scam na dapat mong malaman

Narito ang ilan sa mga pinakakaraniwang uri ng scam para sa iyong kamalayan. Maaari kang makahanap ng karagdagang impormasyon tungkol sa bawat isa sa mga ganitong uri ng scam, kabilang ang mga babalang palatandaan at mga hakbang upang protektahan ang iyong sarili, sa website ng [Scamwatch](#).

Mga scam na pagpapanggap

Lolokohin ka ng mga scammer sa pag-aakala mo na sila ay mula sa mga pinagkakatiwalaang organisasyon tulad ng pulisya, pamahalaan, mga bangko, at mga kilalang negosyo. Maaari rin silang magpapanggap na mga kaibigan o kapamilya. Ang mga scammer ay naghahanap ng impormasyon tungkol sa iyo sa pamamagitan ng pagpapadala ng mga phishing email o mga mensahe. Dinisenyo ang mga ito upang nakawin ang iyong impormasyon. Sinusubukan at kinukumbinsi ka na ibigay sa kanila ang iyong personal na impormasyon sa pamamagitan ng pagpapanggap na sila ay mula sa isang opisyal na organisasyon o isang taong kilala at pinagkakatiwalaan mo.

Gumagamit ang mga scammer ng teknolohiya upang magmukhang galing ang kanilang mga tawag o mensahe sa isang lehitimong numero ng telepono. Maaari nilang palitawin ang mga mensaheng text sa kaparehong thread ng pag-uusap tulad ng mga tunay na mensahe mula sa isang organisasyon.

Mga investment scam

Gumagamit ang mga scammer ng kapani-paniwalang pag-aalok at bagong teknolohiya upang ang kanilang investment proposal ay magmukhang napakaganda kaya't hindi dapat palampasin. Mangangako sila sa iyo ng malaking tubo na may kaunti lamang o walang panganib. Kadalasan silang gumagamit ng mga taktika na pamimilit upang mapakilos ka agad, para madali nilang manakaw ang iyong pera.

Mga scam ng trabaho at pagkaempleyo

Nag-aalok ang mga scammer ng mga trabahong maganda ang sahod at halos walang kahirap-hirap. Nagpapanggap silang nangangalap sa ngalan ng mga kilalang-kilalang kompanya at mga online na shopping platform Kung minsan ang trabahong inilista nila ay hindi talaga totoo. Nagkukunwari rin ang mga scammer na sila ay mga kilalang recruitment agencies.. Ang layunin nila ay nakawin ang iyong pera at personal na impormasyon. Maaaring hilingan kang magbayad muna bago ka makapagtrabaho sa kanila.

Mga scam sa produkto at serbisyo

Magpapanggap ang mga scammer bilang mga mamimili o nagbebenta upang nakawin ang iyong pera. Gumagawa sila ng mga pekeng website o mga profile ng mga lehitimong site ng nagtitinda na nag-aalok ng mga produkto o serbisyo na may mga hindi kapani-paniwalang presyo. Nagpapaskil sila ng mga pekeng patalastas at pekeng review. Maaaring gumagamitsila ng ninakaw na mga logo, isang .com.au na domain name at ninakaw na Australian Business Number (ABN). Ang mga scam na ito ay mahirap mahalata.

Ang mga scammer ay nagpapanggap rin bilang mga negosyo na kilala at pinagkakatiwalaan mo upang magpadala sa iyo ng mga pekeng bayarin. Maaari rin nilang palitan ang mga detalye sa mga lehitimong invoice upang ang mga mamimili ay magbayad sa scammer sa halip na sa iyo.

Mga scam ng pagmamahalan

Ginagamit ng mga scammer ang pangako ng pag-ibig, pag-date, o pakikipagkaibigan upang nakawin ang iyong pera. Talagang nagsisikap silang kumbinsihin ka na ang relasyon ay tunay at manipulahin ka na bigyan mo sila ng pera.

Nahahanap ka ng mga scammer sa social media, mga dating o gaming app at mga website. Maaari rin silang mag-text o mag-email sa iyo. Nagtatago sila sa likod ng mga pekeng profile at pagkakakilanlan, kung minsan ay sa mga kilalang-kilalang tao. Kapag nagtiwala ka na sa kanila, magkakaroon sila ng isang ‘emerhensya’ at hihingi ng tulong sa iyo. Madalas ang mga kahilingan para sa pera o sa iba pang mga produkto.

Mga scam na pananakot at panginigil

Ang mga scammer ay magpapanggap na mula sa isang pinagkakatiwalaang organisasyon at magsasabi na kailangan mong magbayad ng pera o may masamang mangyayari sa iyo. Maaaring takutin ka na aarestuhin, ide-deport, o maging, pisikal kang sasaktan, kung hindi ka sasang-ayon na bayaran sila kaagad.

Maaari ka rin nilang i-blackmail sa pamamagitan ng pagbabanta na ibabahagi nila ang iyong mga ipinadala sa kanila na mga hubad na larawan o video kung hindi ka magpapadala sa kanila ng pera.

Mga scam na hindi inaasahang pera

Susubukan kang kumbinsihin ng mga scammer na mayroong nagkakautang sa iyo o ikaw ay may perang matatanggap o may napanalunang premyo na hindi inaasahan.

Hihilingan ka ng scammer na magbayad ng isang fee o ibigay ang iyong mga detalye ng bangko o pagkakakilanlan bago ka makakolekta ng pera o mga panalo. Sa kasamaang palad, walang libreng pera.





Saan maisumbong ang mga scam

Nagtatrabaho kami upang gawing mas mahirap na target ang Australya para sa mga scammer sa pamamagitan ng pagtataas ng kamalayan tungkol sa kung paano makilala, maiwasan at maisumbong ang mga scam.

Ibinabahagi namin ang impormasyon mula sa mga ulat tungkol sa scam at nakikipagtulungan sa pamahalaan, sa mga nagpapatupad ng batas, at sa pribadong sektor upang buwagin at pigilan ang mga scam.

Tulungan ang iba sa pamamagitan ng pagsusumbong sa Scamwatch. Iulat ang iyong karanasan sa scam sa Scamwatch gamit ang report form sa website ng Scamwatch www.scamwatch.gov.au

Tandaan, kung ikaw ay biktima ng isang scam, mahalagang kumilos kaagad.

- Kung nawalan ka ng pera sa isang scammer, makipag-ugnay sa iyong bangko o card provider.
- Makipag-ugnay sa ID CARE: 1800 595 160 | idcare.org



Karagdagang tulong at suporta

Ang maging isang biktima ng scam ay maaaring nakakapanlumo. Mahalagang tandaan na maaari itong mangyari kaninuman, at may mga suportang makukuha.

Kung ikaw o isang taong kilala mo ay na-scam, makipag-usap sa iba tungkol dito. Maaari kang magpatulong mula sa pamilya, mga kaibigan, iyong GP o isa sa mga sumusunod na serbisyo ng suporta.

Lifeline: 13 11 14 | lifeline.org.au

o suporta sa krisis na chat sa online (24 oras sa isang araw, 7 araw sa isang linggo)

Beyond Blue: 1300 22 4636 | beyondblue.org.au

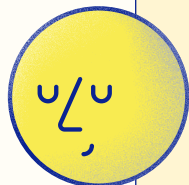
o chat sa online (24 oras sa isang araw, 7 araw sa isang linggo)

Kids Helpline: 1800 55 1800 | kidshelpline.com.au

(24 oras sa isang araw, 7 araw sa isang linggo)

Ang mga epekto ng mga scam sa pananalapi ay nakakapanlumo at nagpapabago ng buhay.

Kung nakararanas ka ng kahirapan sa pananalapi, maaari kang makipag-usap sa isang financial counsellor sa pamamagitan ng **National Debt Helpline: 1800 007 007** mula ika-9:30 ng umaga hanggang ika- 4:30 ng hapon sa Lunes hanggang Biyernes
o mag-Live Chat mula ika-9:00 ng umaga hanggang ika-8:00 ng gabi sa Lunes hanggang Biyernes.



scamwatch.gov.au