# Paano Makikilala at Maiiwasan ang mga Phishing na Scam

Ginagamit ng mga scammer ang email o mga mensaheng teksto upang linlangin ka sa pagbibigay sa kanila ng iyong personal na impormasyon. Ngunit may ilang bagay kang magagawa upang protektahan ang iyong sarili.



## Paano Makikilala ang Phishing

Ginagamit ng mga scammer ang email o mga mensaheng teksto upang linlangin ka sa pagbibigay sa kanila ng iyong personal na impormasyon. Maaaring subukan nilang nakawin ang iyong mga password, numero ng account, o numero ng Social Security. Kung makukuha nila ang impormasyong iyon, maaari silang makakuha ng access sa iyong email, account sa bangko, o iba pang mga account. Naglulunsad ang mga scammer ng libu-libong pag-atakeng phishing na kagaya nito araw-araw — at kadalasan ay matagumpay sila. Iniulat ng Tanggapan para sa Reklamo sa Krimen sa Internet (Internet Crime Complaint Center) ng FBI na ang mga tao ay nawawalan ng $57 milyon sa mga panlilinlang na phishing sa isang taon.
Madalas na binabago ng mga scammer ang kanilang mga taktika, ngunit may ilang palatandaang makakatulong sa iyong makilala ang isang phishing na email o mensaheng teksto.

**Ang mga phishing na email at mensaheng teksto ay maaaring mukhang galing ang mga ito sa isang kumpanyang kilala at pinagkakatiwalaan mo.** Ang mga ito ay maaaring mukhang mula sa isang bangko, kumpanya ng credit card, social networking site, website o app para sa online na pagbabayad, o online na tindahan. **Ang mga phishing na email at mensaheng teksto ay madalas na maglalahad ng kuwento upang linlangin kang mag-click sa isang link o buksan ang kalakip.** Maaari nilang

- sabihing nakapansin sila ng ilang kahina-hinalang aktibidad at mga pagtatangkang mag-log in.
- sabihing may problema sa iyong account o impormasyon sa pagbabayad
- sabihing dapat mong kumpirmahin ang ilang personal na impormasyon
- isama ang isang pekeng invoice
- naising i-click mo ang isang link upang magbayad
- sabihing karapat-dapat kang magparehistro para sa isang refund ng gobyerno
- maghandog ng coupon para sa libreng bagay

Narito ang isang halimbawa sa totoong buhay ng phishing na email.

Isiping nakita mo ito sa iyong inbox. **Nakakakita ka ba ng anumang mga palatandaan na ito ay isang scam?** Tingnan natin.

- Ang email ay mukhang mula sa isang kumpanyang maaaring kilala at pinagkakatiwalaan mo: Netflix. Ginagamit nito pati ang logo at header ng Netflix.
- Sinasabi sa email na naka-hold ang iyong account dahil sa problema sa pagsingil.
- Ang email ay may pangkaraniwang pagbati, "Kumusta," Kung mayroon kang account sa negosyo, maaaring hindi ito gumamit ng pangkaraniwang pagbati na gaya nito.
- Iimbitahan ka ng email na mag-click sa link upang i-update ang iyong mga detalye sa pagbabayad.

Habang sa isang sulyap ay maaring mukhang tunay ang email na ito, ito ay hindi. Ang mga scammer na nagpapadala ng mga email na kagaya nito ay walang kinalaman sa mga kumpanyang pinagpapanggapan nito. Ang mga phishing na email ay maaaring magkaroon ng tunay na kahihinatnan para sa mga taong nagbibigay sa mga scammer ng kanilang impormasyon. At maaari silang magdulot ng pinsala sa reputasyon ng mga kumpanyang ginagaya nila.

## Paano Mapoprotektahan ang Iyong Sarili Mula sa mga Pag-atakeng Phishing

Ang mga spam filter ng email ay maaaring mag-alis sa mga phishing na email sa iyong inbox. Ngunit laging sinusubukan ng mga scammer na malusutan ang mga spam filter, kaya't mabuting ideya ang magdagdag ng karagdagang proteksyon. Narito ang apat na hakbang na maaari mong gawin ngayong araw upang maprotektahan ang iyong sarili sa mga pag-atakeng phishing.

## Apat na Hakbang Upang Maprotektahan ang Iyong Sarili sa Phishing

**1. Protektahan ang iyong computer sa pamamagitan ng paggamit ng panseguridad na software (security software)**. Magtakda upang awtomatikong mag-update ang software nang sa gayon ay tumugon ito sa anumang mga bagong banta sa seguridad.
**2. Protektahan ang iyong mobile phone sa pamamagitan ng pagtatakda upang awtomatikong mag-a-update ang software.** Ang mga update na ito ay makakapagbigay sa iyo ng napakahalagang proteksyon laban sa mga banta sa seguridad.
**3. Protektahan ang iyong mga account sa pamamagitan ng paggamit ng multi-factor authentication.** Ang ilang account ay naghahandog ng karagdagang seguridad sa pamamagitan ng pag-aatas ng dalawa o higit pang kredensyal upang mag-log in sa iyong account. Ang tawag dito ay multi-factor authentication. Ang mga karagdagang kredensyal na kailangan mo upang mag-log in sa iyong account ay napapailalim sa dalawang kategorya:

- Isang bagay na mayroon ka — gaya ng isang passcode na makukuha mo sa pamamagitan ng mensaheng teksto o isang authentication app.
- Isang bagay na likas sa iyo — gaya ng isang scan sa marka ng iyong hinlalaki, iyong retina, o iyong mukha.

Ginagawang mahirap ng multi-factor authentication para sa mga scammer na mag-log in sa iyong mga account kung makukuha nila ang iyong username at password.

**4. Protektahan ang iyong data sa pamamagitan ng pag-back up dito.** I-back up ang iyong data at siguraduhing ang mga backup na iyon ay hindi konektado sa iyong home network. Maaari mong i-copy ang iyong mga file sa computer sa isang external hard drive o cloud storage. I-back up din ang data sa iyong phone.

## Ano ang Gagawin Kung May Pinaghihinalaan Kang Isang Pag-atakeng Phishing

Kung makakakuha ka ng isang email o mensaheng teksto na humihiling sa iyong mag-click sa link o buksan ang isang kalakip, sagutin ang tanong na ito: **Mayroon ba akong account sa kumpanya o kilala ko ba ang taong nakikipag-ugnay sa akin?**
**Kung ang sagot ay "Hindi,"** ito maaaring isang phishing na scam. Bumalik at pag-aralan ang mga tips sa Paano makikilala ang phishing (How to recognize phishing) at tingnan ang mga palatandaan ng phishing na scam. Kung makikita mo ang mga ito, iulat ang mensahe at pagkatapos ay i-delete ito.
**Kung ang sagot ay "Oo,"** makipag-ugnay sa kumpanyang gumagamit ng numero ng telepono o website na alam mong tunay. Hindi ang impormasyon sa email. Ang mga kalakip at link ay maaaring mag-install ng nakakapinsalang malware.

## Ano ang Gagawin Kung Tumugon Ka sa Isang Phishing na Email

Kung sa tingin mo ang scammer ay may impormasyon mo, gaya ng numero ng iyong Social Security, credit card, o account sa bangko, pumunta sa IdentityTheft.gov. Dito, makikita mo ang mga espesipikong hakbang na gagawin batay sa impormasyong nawala mo.
Kung sa tingin mo ay nai-click mo ang isang link o nabuksan ang isang kalakip na nag-download ng nakakapinsalang software, i-update ang security software. Pagkatapos ay i-run ang scan.

## Paano Iuulat ang Phishing

Kung nakatanggap ka ng phishing na email o mensaheng teksto, iulat ito. Ang impormasyong ibinigay mo ay makakatulong na labanan ang mga scammer.

**Hakbang 1.** Kung nakatanggap ka ng phishing na email, i-forward ito sa Grupong Lumalaban sa Phishing (Anti-Phishing Working Group) sa reportphishing@apwg.org. Kung nakatanggap ka ng mensaheng teksto, i-forward ito sa SPAM (7726).
**Hakbang 2.** Iulat ang pag-atakeng phishing sa FTC saFTC.gov/complaint.

May tag ng: cyber security, phishing, scam Mayo 2019