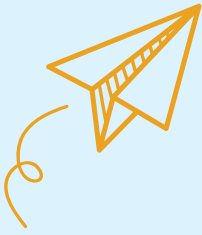


WWW



Mag-ingat:

**Tumigil.
Mag-isip.
Kumonekta.**



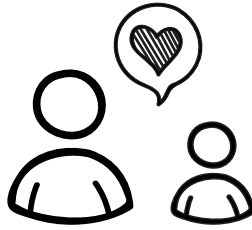
.com

TAGALOG



Mag-click





Para matulungan ang mga bata sa iyong buhay na maging ligtas online, *Ang Mag-ingat: Tumigil. Mag-isip. Kumonekta.* ay may ilang ideya para matulungan kang simulan ang pakikipag-usap sa kanila. Pumili ng seksyon at basahin ito nang magkasama para makita kung paano mag-share nang may pag-iingat, maging mabait online, labanan ang cyberbullying, at protektahan ang kanilang (at ang iyong) personal na impormasyon online. Makakatulong sa iyo ang tools na ito para ipakita sa mga bata kung paano gumawa ng mabubuting desisyon at kung paano gagamitin ang teknolohiya sa responsableng paraan. Gayundin, sa pamamagitan ng pakikipag-usap sa kanila, ipinapaalam mo sa mga bata na mayroon silang mapagkakatiwalaang nasa hustong gulang na makakatulong sa kanila kapag siya ay nagkakamali.

To help kids in your life be safe online, *Heads Up: Stop. Think. Connect.* has some ideas to help you start a conversation with them. Pick a section and read it together to see how to share with care, be kind online, stand up to cyberbullying, and protect their (and your) personal information online. These tools can help you show kids how to make good choices and use technology responsibly. And, by talking with them, you let kids know they have a trusted adult to help them when they make mistakes.

Ang pag-online ay bahagi ng iyong buhay.

Nanonood at gumagawa ka ng content, nagpost ng mga litrato at video, naglalaro ng games, at isini-share ang kinaroonan mo at ang ginagawa mo kasama ang iyong mga kaibigan at pamilya.

Ngunit may mga panganib kapag ikaw ay nagpost, naglalaro, o nakikipag-ugnayan online. Ang ilang tao at sitwasyon na nakakaharap mo ay hindi laging kung ano ang nakikita mo.

Gaano man kabilis tumipa ang iyong mga daliri sa keyboard, phone, o tablet, ang pinakamainam na tools na mayroon ka para maiwasan ang mga panganib online ay ang iyong utak at panahon.

Tumigil at pag-isipan ang mga sitwasyon para matulungang maprotektahan ang iyong sarili, ang iyong mga kaibigan, ang iyong mga account, at ang iyong mga device. Kung hindi ay baka mauwi ka sa labis na pag-share, panghihiya sa iyong sarili o sa iba, magkamali sa iyong computer, o makipag-usap sa mga taong nagpapanggap na iba.



MAG-SHARE NANG MAY PAG-IINGAT



COOL ANG MAGING MABAIT



LABANAN ANG CYBERBULLYING



ANG KONEKSYON SA PROTEKSYON

MAG-SHARE NANG MAY PAG-IINGAT



Mag-isip bago ka mag-share

Ang ginagawa mo online ay may mga tunay na konsekuwensiya. Ang mga litrato, video, at mensaheng isini-share mo ay makakaapekto sa iyo, sa iyong pagkapribado, sa iyong reputasyon, at sa mga taong nasa paligid mo — sa kasalukuyan at sa hinaharap. Tumigil at mag-isip bago ka mag-post.

Ang ipino-post mo ay maaaring magkaroon ng mas maraming “tagatingin” kaysa sa iniisip mo.

Imposibleng ganap na makontrol kung sino ang makakakita sa iyong profile, mga litrato, mga video, o mga text — kahit kung gumagamit ka ng mga privacy setting o app na bumubura sa iyong content

pagkatapos itong makita o sa loob ng 24 na oras. Ang sinumang nakakakita sa iyong post ay maaaring kumuha ng screenshot o recording. Itanong sa iyong sarili: "Gugustuhin ko bang tumayo sa gitna ng oras ng tanghalian at i-share ang litrato o video na iyon sa buong cafeteria?"

Ang isini-share mo ay maaaring makaapekto sa iba.

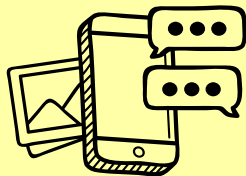
Maaaring nakakahiya, hindi patas, at hindi ligtas na magpadala o mag-post ng mga litrato o video nang hindi kumukuha ng pahintulot mula sa mga taong naroon. Kunin muna ang pahintulot ng iba. Bago ka mag-post, itanong sa kanila: "Okey ba sa iyo kung ipo-post ko ito sa social?" Kung humindi sila, huwag itong i-post.

Sa oras na mag-post ka ng isang bagay online, hindi mo na ito mababawi

Kahit i-delete mo pa ang isang bagay na nai-post mo — o mag-expire ang post — ang litrato o komentong iyon na ayaw mo nang makita ng mga tao ay maaaring mai-save, mai-share, o manatili sa ibang lugar online — nang permanente.

Sexting: Huwag itong gawin

Maaaring may narinig kang mga kuwento sa paaralan o sa balita tungkol sa mga taong ginagawa ang “sexting” — nagpapadala ng mga hubad na litrato mula sa kanilang mga phone. Huwag itong gawin. Tapos. Inilalagay sa panganib ng paggawa, pagpapadala, o maging pag-save ng mga hayagang sekswal na litrato, video, o mensahe ang iyong mga pagkakaibigan at reputasyon. At ang mas masama, maaaring lumalabag ka sa batas.



Ang dapat tandaan tungkol sa social media



Ayon sa U.S. Surgeon General, maaaring makasama sa iyo ang paggamit ng social media, depende sa kung gaano kahabang oras ang ginugugol mo sa mga platform, uri ng content na nakikita mo, at kung gaano ito nakakagambala sa mga bagay-bagay tulad ng iyong pagtulog o ehersisyo — mga aktibidad na iyon na mahalaga para sa iyong kalusugan.

COOL ANG MAGING MABAIT



Mahalaga ang pagiging magalang



Kapag hindi mo nakikita online ang ekspresyon ng mukha, kilos ng katawan, o iba pang makikitang palatandaan sa isang tao, maaaring hindi ka mag-atubiling mag-post o magsabi ng mga bagay na hindi mo masasabi nang personal. Ngunit ang pagte-text, pagpo-post, direktang pagpapadala ng mensahe, paglalaro ng video games, at pag-email ay katulad ng pakikipag-usap sa isang tao nang harap-harapan. Maging maingat sa kung paano ka nakikipag-usap at mag-isip bago ka magsalita o mag-post.

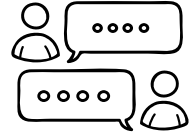
Magdahan-dahan. Madaling magkaroon ng hindi pagkakaunawaan online. Bago ka magpadala ng mensahe, itanong sa iyong sarili: "Ano ang mararamdaman ng ibang tao sa mensaheng ito?"

Isaalang-alang at igalang ang mga pananaw at nararamdaman ng ibang tao online — tulad ng gagawin mo sa personal. Tandaan: may mga tunay na tao sa likod ng mga avatar at pangalan ng profile.

Maging malumanay. Huwag isulat ang lahat sa **MALALAKING TITIK**, mahahabang hanay ng tandang padamdang, o malalaking font na naka-bold. Katulad ito ng pagsigaw.

Huwag isulat ang lahat sa group chat.

Bago mo ipadala ang isang mensaheng panggrupo o pindutin ang Reply All, tumigil at mag-isip: Sino ang kailangang makakita ng mensaheng ito?



Huwag magpanggap

Mali at posibleng makasama ang gumawa ng mga profile, komento, o post na mukhang nanggagaling sa iba, tulad ng isang indibidwal sa iyong klase o guro.

Magsalita

Kung may nakita kang kaibigan na nag-post ng isang bagay na hindi pinag-isipan o hindi ligtas, sabihin sa kanila. Maaaring mapaiwas mo ang iyong kaibigan sa problema o sa pagkakapahiya sa kanyang sarili. Kung may nakita kang isang bagay na hindi nararapat online, i-report ito at ipaalam sa isang pinagkakatiwalaang nasa hustong gulang. Karamihan sa mga app at platform ay may paraan para mag-report kung ang pag-uugali ng isang tao ay nagbabanta o hindi nararapat.



*Maging
Mabait!*



LABANAN ANG CYBERBULLYING



Ang bawat isa ay nararapat na maramdamang siya ay ligtas sa kanyang mga pang-araw-araw na interaksyon sa ibang tao, ito man ay online o harap-harapan.

Kung may isang taong nag-post ng masasamang komento, nakakasakit na meme, nakakahiyang litrato, o nagpadala ng mga chat o pribadong mensahe tungkol sa iyo, iyon ay pambu-bully. Hindi ito okey. Makipag-usap sa isang pinagkakatiwalaang nasa hustong gulang para makakuha ng tulong sa sitwasyon at magpasya kung paano ka dapat tumugon.

Kung may nangharas sa iyo online, narito ang dapat gawin:



Huwag pansinin ang taong iyon o i-block siya para hindi ka na niya kontakin pa.



I-save ang mga rekord at humingi ng tulong mula sa isang pinagkakatiwalaang nasa hustong gulang.



I-report ito. Maraming app at platform ang may tools para i-report ang isang tao dahil sa pag-uugaling hindi nararapat o nagbabanta.

Ang pambu-bully ay madalas na nagpapasama sa nararamdaman ng taong nahaharas — at mukhang pinasasama nito ang nambu-bully.

Sa pambu-bully ay maaari ka ring magkaroon ng problema sa iyong paaralan o sa pulis.

Kung nakakasaksi ka ng cyberbullying, maghanap ng mga paraan para maging isang tagapagtanggol — isang taong nakikialam, gumagambala, o nagsasalita para maitigil ang pambu-bully. Ang masamang pag-uugali ay madalas na tumitigil agad kapag may nagtatanggol sa taong binu-bully.

ANG KONEKSYON SA PROTEKSYON



Protektahan ang iyong privacy

Kapag may ginagawa kang anumang bagay online, nag-iiwan ka ng bakas. Gawin ang mga hakbang na ito para matiyak na ang bakas ay hindi nagreresulta sa impormasyong maaaring hindi mo nilalayong i-share.

Gamitin ang privacy settings. Alamin kung paano pagaganahin ang privacy settings para sa mga device, app, at account sa social media — pagkatapos ay gawin ito. Natutulungan ka nitong limitahan kung sino ang nakakakita sa kinaroroonan mo, sa ipino-post mo, at sa kung sino ang kumukonekta sa iyo.

Tingnan ang iyong location settings. May ilang app na nagpapahintulot sa iyong makita kung nasaan ang mga kaibigan mo. Isini-share din nito kung nasaan ka. Pag-isipan kung kailan makatuwiran na mag-share ang iyong lokasyon. Kapag hindi, i-off ang pag-share ng lokasyon. Ang mga

feature sa iyong mga device, tulad ng camera, ay maaaring magkaroon ng impormasyon tungkol sa kung nasaan ka noong kinuha mo ang litrato. Kung ayaw mong i-broadcast kung nasaan ka sa bawat selfie, i-off ang iyong lokasyon sa camera ng iyong phone. Laging itanong sa iyong sarili: "Kailangan bang malaman ng app na ito kung nasaan ako?"



Limitahan ang iyong mga online na kaibigan sa mga taong kilala mo talaga. Maaaring nakakatuwa ang kumonekta sa mga kaibigan sa pamamagitan ng text, social media, o video games — ngunit may mga taong nagpapanggap na hindi sila online. At kung hindi ka nag-iingat, maaari kang magbahagi ng personal na impormasyon sa isang estranghero.

Protektahan ang iyong impormasyon

Sa oras na maibigay mo ang iyong personal na impormasyon — tulad ng iyong Social Security number, mga password, o impormasyon ng account sa bangko — sa isang taong hindi mo kilala, wala nang paraan para mabawi pa ito.

Narito ang paraan para maprotektahan ang iyong impormasyon online:

Huwag mag-reply sa mga mensaheng humihingi ng personal na impormasyon. Kahit na kung ang mensahe ay mukhang galing sa isang kaibigan, miyembro ng pamilya, o kumpanyang kilala mo — o nagsasabing may masamang mangyayari kung hindi ka magre-reply. Malamang na peke

ito at ipinadala para nakawin ang iyong impormasyon. Magpatulong sa isang pinagkakatiwalaang nasa hustong gulang para i-report ang mensahe bilang junk o spam.

Tingnan kung anong impormasyon ang gustong i-access ng app — bago mo ito i-download. Ang ilang app ay humihingi ng pahintulot na i-access ang impormasyon o mga feature na hindi nila kailangan, tulad ng listahan ng iyong kinokontak, camera, storage, lokasyon, at microphone. Humingi ng tulong sa isang pinagkakatiwalaang nasa hustong gulang sa pagbabasa ng patakaran sa pagkapribado ng app para makita kung paano magagamit ang iyong data at kung ito ay ise-share. Pagkatapos ay magpasya kung kailangan talaga ng word game na i-access ang iyong mga litrato.

Makipag-usap sa isang pinagkakatiwalaang nasa hustong gulang bago gumawa ng mga pagbili sa app— lalo na kung sila ang magbabayad sa mga ito.

Protektahan ang iyong mga account

Nagtatabi ka ng maraming personal na impormasyon sa iyong mga online account. Narito ang ilang hakbang na gagawin para ilayo ang iyong mga account sa ibang tao.

Gumawa ng matitibay na password.

Mas mahirap maunawaan kung mas mahaba ang iyong password. Gumamit ng hindi bababa sa 12 karakter na may magkakahalang malalaki at maliliit na titik, numero, at simbolo. Isaalang-alang ang paggamit ng passphrase ng mga random na salita para gawing mas matatandaan ito.

Ngunit huwag gumamit ng mga karaniwang parirala, liriko ng kanta, o sinabi sa pelikula na madaling mahulaan.

Maging katangi-tangi. Gumawa ng magkakaibang password para sa iba't ibang account mo. Sa ganoong paraan, kung may nakakuha ng password para sa isang account, hindi niya ito magagamit para makapasok sa iba mo pang mga account. Ang isang paraan para masubaybayan ang lahat ng magkakabang password ay ang paggamit ng password manager.

Panatilihin itong pribado. Huwag ibahagi ang iyong mga password sa kahit sino, kahit sa pinakamatalik mong kaibigan o sa iyong katipan.

Maging mapili sa mga tanong na panseguridad. Subukang



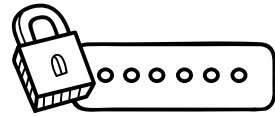
piliin ang mga tanong na panseguridad na ikaw lang ang makakasagot. Laktawan ang mga tanong na may mga sagot na mahahanap ng sinuman online — tulad ng iyong zip code, lugar ng kapanganakan, o apelyido sa kadalagahan ng ina. Kung hindi mo maiiwasan ang mga tanong na iyon, maging malikhain! Tratuhin ang mga ito na tulad mga password at gumamit ng mga random at mahahabang sagot. Siguraduhin lang na matatandaan mo ang iyong mga sagot.

Gumamit ng multi-factor authentication. Maraming account ang nagbibigay ng dagdag na proteksyon sa iyong mga account sa pamamagitan ng paggamit ng “multi-factor authentication” — na humingi ng isang bagay bukod sa

password lamang. Isinasama ng multi-factor authentication ang isang bagay na alam mo (tulad ng password) sa isang bagay na mayroon ka (tulad ng passcode na inilabas ng app) o isang bagay na ikaw (tulad ng fingerprint).

Agad na palitan ang mga password kung may paglabag.

Kung sinabi sa iyo ng kumpanya na nagkaroon ng paglabag sa data kung saan maaaring nakuha ng isang hacker ang iyong password, baguhin agad ang password na ginagamit mo sa account na iyon. Baguhin din ito para sa anumang account na gumagamit ng katulad na password.



Protektahan ang iyong mga device

Ang pinakamahasag na paraan para masiyahan sa pag-online? Pagtitiyak na ang iyong mga device ay ligtas at may seguridad. Magsimula rito.

I-set ang security software para awtomatikong mag-update para sa lahat ng iyong device, internet browser, at operating system. Tinutulungan ka nitong magprotekta laban sa mga bagong banta sa seguridad.

Huwag mag-click ng mga link o magbukas ng mga attachment. Kung nakatanggap ka ng hindi inaasahang text, email, o mensahe online na nagsasabi sa iyong mag-click sa isang link o magbukas ng attachment, huwag itong gawin! Kahit ito ay isang alok para sa libreng bagay. Ang mga link at attachment ay maaaring magkubli ng mga virus o spyware na maaaring makasira sa iyong phone, computer, o tablet.

Protektahan ang iyong mga device gamit ang password. Makakatulong itong maiwasan ang pagpunta sa maling kamay ng iyong mga litrato, mensahe, at account.

Itabi ang mga ito sa isang ligtas na lugar. Ito man ay iyong phone, laptop, o tablet, huwag itong iwan sa publiko — kahit isang sandali lang.

Alamin pa sa



This booklet helps kids socialize safely online. There's help on how to share with care, be kind online, stand up to cyberbullying, and protect their personal information. Get free copies in English or Spanish at

ftc.gov/bulkorder



**FEDERAL TRADE
COMMISSION**

Agosto 2023