Mga Scam at ang Iyong Maliit na Negosyo:

Isang Gabay Para sa Pagnenegosyo

Tagalog

Kapag nagtangka ang mga scammer sa iyong negosyo o non-profit na organisasyon, maaari nitong masira ang iyong reputasyon at ang iyong kita. Ano ang pinakamagandang proteksyon mo? Alamin ang mga palatandaan ng panloloko na pumupuntirya sa mga negosyo. Pagkatapos ay sabihin sa iyong mga empleyado at kasamahan ang mga dapat alamin upang sila ay makaiwas sa mga panloloko.

- **Mga Pamamaraan ng mga Scammer**
- **Protektahan ang Iyong Negosyo**
- **Mga Karaniwang Scam na ang Target ay Maliliit na Negosyo**
- **Iba pang mga Kahina-hinalang Gawain**

▶ Mga Pamamaraan ng mga Scammer

- **Ang mga scammer ay nagpapanggap na sila ay iyong pinagkakatiwalaan.** Nagpapanggap silang isang kompanya o ahensya ng gobyerno na alam mo para ikaw ay kanilang mapagbayad. Ngunit ito ay isang scam.
- **Ang mga scammer ay lumilikha ng pakiramdam ng pagmamadali, pananakot, at pangamba.** Ang gusto nila ay umaksyon ka agad bago mo makuha ang kanilang claims. Huwag mong hayaan na madaliin kang magbayad o magbigay ng sensitibong impormasyon na pangnegosyo.
- **Ang mga scammer ay humihingi ng bayad sa espesipikong mga paraan.** Kadalasan, humihingi sila ng bayad sa pamamagitan ng wire transfer, cryptocurrency, o gift card. Huwag kang magbayad sa sinumang humihingi ng bayad sa mga ganitong paraan. Ito'y isang scam.

▶ Protektahan ang Iyong Negosyo

Sanayin ang Iyong Tauhan

- Ang iyong pinakamahusay na depensa ay ang mga tauhang may kamalayan. Sanayin ang iyong tauhan na huwag magbigay ng password o sensitibong impormasyon sa email, kahit ang email ay mukhang galing sa isang manager. Ipaliwanag sa iyong tauhan kung paano nagagaganap ang mga scam at hikayatin silang makipag-usap sa kanilang katrabaho kung may pinaghihinalaan silang scam. Kumuha ng mga libreng kopya ng brochure sa **ftc.gov/bulkorder** at ibahagi ang mga ito sa iyong mga tauhan.

I-verify ang mga Resibo at mga Bayarin

- Siguraduhin malinaw ang mga hakbang para sa pag-apruba ng mga pinamili at resibo, at hilingin din sa iyong tauhan na tiyaking wasto ang lahat ng resibo. Bigyang-pansin kung paano humihingi ng bayad ang isang tao at sabihin din sa iyong mga tauhan na gawin din ang bagay na ito. Kung may humiling na magbayad ka sa papamagitan ng wire transfer, cryptocurency, o gift card, huwag kang magbayad. Scam iyon.

Hanapin ang mga Tech-Related Scam

- Dahil madalas na pinepeke ang kanilang phone number, huwag magtiwala sa caller ID. Kung may natanggap kang text message o email, huwag pindutin ang anumang link, magbukas ng mga attachment o mag-download ng mga file. Sa ganiyang paraan naglalagay ng malware ang mga scammer sa iyong network o susubukan kang kumbinsihin na magpadala ng pera o magbahagi ng mga sensitibong impormasyon. Ang mga scammer ay madalas mang-hack ng mga social media account ng mga taong kilala mo, at magpapadala ng mga mensaheng mukhang totoo — pero hindi. Matuto nang higit pa tungkol sa pagprotekta sa iyong maliit na negosyo o non-profit na organisasyon mula sa mga cyber scammer at hacker: tingnan ang **Cybersecurity para sa Maliit na Negosyo** sa **ftc.gov/cybersecurity**.

Kilalanin Kung Sino ang Iyong Kinakausap

- Bago makipagnegosyo sa mga bagong kompanya, hanapin ang pangalan ng kompanya na may kasamang term na “scam” o “reklamo.” Basahin ang iba pang mga komento tungkol sa kompanya. Magtanong sa mga taong pinagkakatiwalaan mo para sa kanilang mga

mungkahi. Maaari ka ring makakuha ng libreng paalaala para sa ikauunlad ng negosyo at payo sa pamamagitan ng mga programa tulad ng **SCORE.org**.

▶ Mga Karaniwang Scam na ang Target ay Maliliit na Negosyo

Pekeng Resibo at mga Produktong Hindi Inorder

Ang mga scammer ay gumagawa ng pekeng resibo na mukhang ikaw ay umorder ng produkto o serbisyo para sa iyong negosyo. Inaasahan nila na maniniwala ang taong magbabayad ng iyong invoice na totoo ang resibo at magbabayad. Pero peke ito. O maaaring tumawag ang scammer na gusto niyang "kumpirmahin" ang iyong order, "i-verify" ang iyong tirahan, o magbigay ng "libreng" catalog o sample. Kung sasagot ka ng oo sa alinman sa mga iyon, ang produktong hindi inorder ay darating sa iyong pintuan — na may malaking halaga na dapat mong bayaran. Huwag magbayad. At tandaan, kapag nakatanggap ka ng produkto na hindi mo inorder, may legal kang karapatan kunin ito at at hindi bayaran.

Online Listing and Mga Advertising Scam

Ang mga scammer ay susubukang lokohin ka na mapagbayad sa mga nonexistent advertising o listing sa mga phony business directory. Hihingan ka nila ng iyong contact information para sa "libreng" listing, o sasabihin na ang tawag at para "kumpirmahin." Sa ibang pagkakataon, makakakuha ka ng malaking bill, at maaaring gumamit ang scammer ng mga detalye — o recording — ng mga naunang tawag para pilitin kang magbayad.

Mga Scam na Nanggagaya ng Negosyo o Tagagobyerno

Ang mga scammer ay magpapanggap na kakilala mo o pinagkakatiwalaan at susubukan ka nilang takutin o pagbayarin ka agad para bigyan mo sila ng impormasyon. Halimbawa:

- Ang mga scammer ay magsasabing tumatawag sila mula sa isang utility company para sabihing mapuputulan ka na ng gas, kuryente, o serbisyo sa tubig dahil sa (hindi totoong) late bill.
- Ang mga scammer ay nagsasabing sila ay ahente ng gobyerno at babantaan kang sususpindihin ang iyong lisensiya sa negosyo, pagmumultahin ka o idedemanda. Sasabihin nila na may babayaran ka kasing buwis o kailangan mong mag-renew ng lisensya o rehistro.
- May mga scammer na kukumbinsihin kang bumili ng mga workplace compliance poster na maaari mong makuha nang libre galing sa U.S Departmer of Labor.
- Ang mga ibang scammer ay lolokohin kang magbayad para i-apply ang mga kaloob na negosyo kuno na galing sa programa ng gobyerno na hindi pala totoo.
- Ginagaya ng mga scammer ang U.S Patent at Trademark Office at nagbabanta na mawawala ang iyong trademark kung hindi ka kaagarang magbabayad sa kanila. Minsan, sila ay nagsisinungaling at nagsasabing ikaw ay may dapat bayaran sa mga karagdagang rehistro sa mga serbisyon.
- Ang ibang mga scammer ay tumatawag sa mga tech company, sila ay nagbabanta na mawawala ang kanilang website URL kung hindi ka agad magbabayad.

Mga Scam ng Tech Support

Ang mga scam ng tech support ay nagsisimula sa isang tawag o isang nakaka-alarmang pop-up na mensahe

sa iyong screen. Ang mga scammer ay nagkukunwari na galing sa isang kilalang kompanya ng tech, na nagsasabing may problema sa seguridad ng iyong computer. Ang kanilang layunin ay makuha ang iyong pera, makapasok sa iyong computer, o parehas. Maaari ka nilang pagbayarin sa pag-aayos ng isang problema na wala ka naman talaga, ilista ang iyong negosyo sa isang hindi umiiral o walang silbing computer maintenance program, o palihim na pumasok sa iyong computer network upang kunin ang mga kompidensyal na data na maaari nilang gamitin upang magnakaw ng pagkakakilanlan.

Social Engineering, Phishing, at Ransomware

Ang mga cyber scammer ay maaaring manloko ng mga empleyado para magpadala sa kanila ng pera o magbigay ng kanilang kompidensyal o sensitibong impormasyon katulad ng password o bank information. Kadalasan itong nagsisimula sa isang phishing email, social media contact, o sa isang tawag na tila nanggaling sa isang pinagkakatiwalaang pinagkukunan — halimbawa, isang supervisor o iba pang matatandang empleyado — na nagmamadali o nananakot. Ang iba pang mga email ay maaaring magmukhang rutin na pagpapalit ng password o iba pang automated na mensahe, pero ang totoo, gusto nilang nakawin ang iyong impormasyon. Ang mga scammer ay maaari ding gumamit ng malware upang i-lock ang mga file ng mga organisasyon at hawakan ang mga ito kung hindi sila bibigayan ng ransom.

Mga Scam sa Pagtuturo ng Pagnenegosyo

Ang iba pang mga scammer ay nagtitinda ng mga bogus na programa sa pagtuturo sa negosyo, kadalasan ay gumagamit ng mga pekeng patotoo, video, seminar presentation at telemarketing call. Nangangako sila ng mga nakamamanghang resulta kapag ikaw ay nagbayad

para sa kanilang ekslusibong “napatunayan” na sistema upang magtagumpay ang iyong negosyo. Maaari ka rin nilang akitin na mababa lang ang una mong ilalabas, pero hihingan ka ng libo-libong dolyar kalaunan. Sa katunayan, iniiwan ng mga scammer ang mga negosyanteng nagsisimula pa lang na may libo-libong utang.

Pagbabago ng mga Online Review

Ang ibang scammer ay nagsasabing kaya nilang palitan ang mga negatibong review sa iyong produkto at serbisyo, makadagdag ng mga positibong review o palakasin ang iyong puntos sa mga ratings site. Gayunpaman, ang pag-post ng mga pekeng review ay ilegal. Sinasabi ng mga tagubilin ng FTC na ang mga pag-endorso — kasama ang review — ay dapat magpakita ng tapat na opinyon at karanasan ng mga tagapag-endorse.

Mga Scam sa Pagproseso ng Credit Card at Pag-upa ng Kagamitan

Ang ibang scammer ay nangangako ng mas mababang halaga sa pagproseso ng mga transaksyon sa credit card o mas magandang mga deal sa pag-upa ng kagamitan. Ang mga scammer na ito ay gumagamit ng fine print, half-truth, at flat-out na mga kasinungalingan para mapapirma ang isang may-ari ng negosyo sa isang kontrata. Ang ilang walang prinsipyong ahente ay humihiling sa mga may-ari ng negosyo na lumagda sa mga blankong dokumento. (Huwag itong gawin.) Ang iba ay kilala na nagbabago ng mga napagkasunduan pagkatapos ng usapan. Tanungin ang sales person na bigyan ka agad ng kopya ng lahat ng dokumento. Kung sakaling tumanggi sila o sabihing saka na lang ito ipapadala, maaaring palatandaan ito na scammer ang kausap mo.

Mga Scam ng Pekeng Tseke

Ang ibang scammer ay magbibigay sa iyo ng tila kapani-paniwalang rason na babayaran ka nang sobra gamit ang tseke. Sumunod, hihikayatin ka na ibalik sa kanila o sa ibang tao ang ekstrang pera. Pero peke ang tseke, kahit na ang makikita sa iyong account ay “cleared.” Sa oras na makita ng bangko na ang talbog ang tseke, nasa kamay na ng scammer ang perang ipinadala mo. Mapipilitan kang bayarang muli ang bangko.

► Iba pang mga Kahina-hinalang Gawain

Minsan, nagtatago ang mga scammer sa ibang kahina-hinalang gawain — katulad ng pag-aangking magbibigay ng trabaho na malaki ang kita, pero naman kayang patunayan ang kanilang mga binitiwang pangako. O maaaring ikaw ay bentahan ng mga hindi na kailangang serbisyo kasama na inaangking kailangan mong magbayad upang mapabuti ang ulat sa credit ng negosyo mo. At pagkatapos na tumama ang likas na sakuna, ang mga hindi lisensiyadong mangongontrata at mga manloloko ay maaaring magpakita at mangakong ibabangon nila agad ang negosyo mo sa pamamagitan ng madaliang pag-aayos, paglilinis, o pagtanggal ng dumi na hindi naman nangyari.

▶ Matuto Nang Higit Pa

- Para sa karagdagang kaalaman sa pagprotekta ng iyong organisasyon laban sa mga panloloko, bisitahin ang **ftc.gov/SmallBusiness**.
- Manatiling konektado sa mga FTC sa pamamagitan ng pag-subscribe sa mga Business Blog ng FTC sa **ftc.gov/subscribe**.

▶ Iulat Ito

- Kung aktwal kang nakakita ng scam, tumawag sa 877-382-4357, at pindutin ang 3 para sa iba pang mga wika, at pagkatapos ay 2 para sa Tagalog — o magpunta sa **ReportFraud.ftc.gov**.
- Abisuhan ang iyong Pangkalahatang Abugado ng estado. Maaaring makita ang contact information sa **NAAG.org**.

▶ Makibahagi

- Tandaan: Ang iyong pinakamahusay na depensa ay ang mga manggagawang may kamalayan. Kausapin ang iyong mga tauhan tungkol sa kung paano nangyayari ang mga panloloko.
- Ibahagi ang brochure sa iyong manggagawa.
- I-download ang libreng kopya nitong brochure sa **ftc.gov/languages**.

Tungkol sa FTC

Nakikipagtulungan ang FTC sa mga may-ari ng maliliit na negosyo upang maiwasan ang mga scam, protektahan ang kanilang mga computer at network, at panatilihing ligtas ang data ng kanilang mga customer. Para mahanap ang impormasyon para sa mga maliliit na negosyo, magpunta sa **ftc.gov/SmallBusiness.** Makakahanap ka roon ng impormasyon tungkol sa mga scam na nagta-target ng maliliit na negosyo at kung paano maiiwasan ang mga ito, at impormasyon sa cybersecurity para sa maliliit na negosyo para matulungan ang mga may-ari na panatilihing ligtas ang kanilang mga network.

Para makakuha ng pinakabagong impormasyon para sa maliliit na negosyo, mag-subscribe sa FTC's Business Blog sa **ftc.gov/subscribe**.

This brochure is part of the FTC's efforts to help small business owners avoid scams. It explains common scams that target small businesses and non-profit organizations, describes scammers' tactics, and provides steps business owners can take to protect their company from scams. Order print copies for free at **ftc.gov/bulkorder**.

FEDERAL TRADE COMMISSION

business.ftc.gov

Hulyo 2023