



CHARITY SCAMS

You may see charities that you don't recognize asking for donations in the wake of COVID-19.

TAKE ACTION

If you donated to a fraudulent charity, visit <u>FightCybercrime.org</u> for recovery help.

Verify all charities before donating on the IRS tax exemption site.



ONLINE SHOPPING SCAMS

Cybercriminals may try to sell you bogus COVID-19 vaccinations and home test kits.

TAKE ACTION

If you have purchased a fake vaccine or home test kit, visit FightCybercrime.org for recovery help.

Visit the <u>Federal Trade Commission</u> to learn more about companies selling fake coronavirus treatments.



PHISHING SCAMS

Emails impersonating the World Health Organization, the CDC, and other reputable sources may hit your inbox. These emails may ask you to click a link or share your sensitive information.

TAKE ACTION

If you've clicked on a phishing link or shared personal information, visit <u>FightCybercrime.org</u> for recovery help.



ROBOCALLS

Calls from cybercriminals pretending to be government organizations, family members in distress, or banks/credit card companies are on the rise. These calls will often ask for gift cards as payment.

TAKE ACTION

If you have provided personal information to a robocaller, visit <u>FightCybercrime.org</u> for recovery help.



ROMANCE SCAMS

Cybercriminals will try to capitalize on the heightened internet traffic to lure people into romance scams.

TAKE ACTION

If you find yourself involved in a romance scam, visit FightCybercrime.org for recovery help.

They will often ask for gift cards for medical expenses or bills.



SOCIAL MEDIA SCAMS

Social media is a tool that cybercriminals use to distribute false information and capitalize on panic.

TAKE ACTION

If you're looking for information on social media, visit trusted profiles like the <u>CDC</u>, <u>World Health Organization</u>, <u>Federal Trade Commission</u>, and the Better Business Bureau.







