# Coronavirus stimulus scams are here. How to identify these new online and text attacks

COVID-19 fears are fertile ground for malicious actors. Here's how to stay safe online.

As with any public crisis, the spread of the coronavirus has created a new crop of hackers -- targeting people who are awaiting their stimulus check, who are working from home and who are just trying to stay healthy. Add in April Fools' Day and you need to be on guard against all kind of scams and misinformation found online, in your email inbox and even in your text messages.


A recent release from the FBI's Internet Crime Complain Center offers some solid advice on what to watch out for.

"Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them," the FBI said. "Protect yourself and do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits."

## Here phishy, phishy

Unsolicited emails that prompt you to click on an attachment should always raise a red flag when you're checking your inbox. But these classic email phishing scams still lure unsuspecting users into downloading malicious items and giving up their login information every day.

With the news that the government is going to issue payments of up to $1,200 in coronavirus relief to US taxpayers in the coming month, the FBI recently issued a warning to be on alert for attackers masquerading as the agency and asking for personal information supposedly in order to receive your check. "While talk of economic stimulus checks has been in the news cycle, government agencies are *not* sending unsolicited emails seeking your private information in order to send you money," the warning said.

Among other steps to create a safer inbox, the US Cybersecurity and Infrastructure Security Agency recommends turning off your email client's option to automatically download attachments. Not all email clients offer this and each client is different, but some do. Because social engineering attacks -- scams designed to persuade you to hand over your sensitive information by targeting specific information about you -- have become increasingly common in times of crisis, it's also a good idea to read up on how to identify these security risks.

And remember, never reveal personal or financial information in an email, or respond to requests for it.

## Mobile malware

If you're looking to track COVID-19 news with an app, it's a good idea to keep an eye out for malware traps. Earlier in March, a malicious Android app called CovidLock claimed to help users chart the spread of the virus. Instead, it led to a slew of Android phones being locked and held for ransom by hackers.

Meanwhile, Reason Labs recently discovered hackers were using coronavirus-tracking map sites to inject malware into people's browsers. As reported by Market Watch, coronavirus-related website name registrations are 50% more likely to be from malicious actors.

As Android Authority points out, setting a password on your phone can help protect you from a lock-out attack if you're using Android Nougat. It's also a good idea to stick to the Google Play store for any coronavirus-related apps to better your odds of installing benign software.

## Charity check-out

During a disease outbreak or natural disaster, the better angels of our nature compel us to open our wallets to the less fortunate through charitable giving and donation. Before we follow that impulse, we need to take an extra few moments to make sure the charity isn't a funnel into the bank account of a predatory impersonator.

Taking a few moments to review the Federal Trade Commission's Charity Scams page could save you the heartbreak of an emptied checking account. You can also improve your odds by searching sites such as guidestar.org and give.org for the name of your charity before donating.

## Legit sources

Random Facebook groups offering supposed home cures for COVID-19, long Twitter threads from self-appointed health experts and cleverly designed websites -- there are dozens of ways misinformation can lure

unsuspecting victims into a position of vulnerability. While it can be hard to sort the solid information from the scam-baiting, here are a couple of ways:

1. By clicking the "about" section of a Facebook group, you can see whether that group has changed its name multiple times to reflect new national crises -- a sure sign that the group is trawling for an audience rather than promoting reliable news.
2. Keep an eye on official sources on Twitter, including the accounts of trusted news sites and their news reporters, and avoiding political operatives where possible.
3. If a site claims to be an official government publication, check the URL to see if it ends in .gov.