lobo INTERNET SERVICES LTD.

Newsletter

May 2020

AVOID CORONAVIRUS SCAMS

Don't respond to texts, emails or calls about checks from the government. The details are still coming together.

Ignore online offers for vaccinations. There are no products proven to treat or prevent COVID-19 at this time.

Be wary of ads for test kits. The FDA just announced approval for one home test kit, which requires a doctor's order. But most test kits being advertised have not been approved by the FDA, and aren't necessarily accurate.

Hang up on robocalls. Scammers are using illegal robocalls to pitch everything from low-priced health insurance to work-at-home schemes.

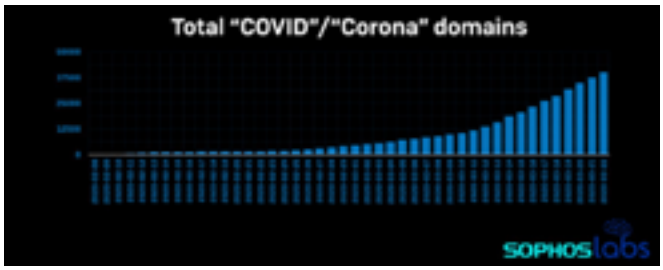
Watch for emails claiming to be from the CDC or WHO. Use sites like coronavirus.gov and usa.gov/coronavirus to get the latest information. And don't click on links from sources you don't know.

Do your homework when it comes to donations. Never donate in cash, by gift card, or by wiring money.

SOPHOS Antivirus

Common attack techniques plus three practical steps to help minimize risk.

Hackers are busy exploiting coronavirus in their attacks. In recent weeks SophosLabs has seen a surge of COVID- and Corona-related domains registered – while some will be legitimate, it's a fair bet that the majority are destined for criminal purposes.



Common attack techniques

Phishing attacks using COVID-19 as a lure are the most visible and immediate cybersecurity risk right now. Common tactics include:

Coronavirus news

Beware of emails, SMS, and WhatsApp messages from unknown sources with information on coronavirus. Often hackers impersonate legitimate organizations and people to make their messages more believable.

Home delivery scams

With many people waiting on home delivery of essential items, hackers are impersonating delivery services. Their goal: to trick you into clicking malicious links or con you into paying extra 'delivery' fees.

We're also seeing coronavirus used in other ways, including:

Extortion attempts

Criminals threaten to infect people with coronavirus unless you pay them. Often these threats include a small piece of personal information to make it more believable.

Malicious apps

Purporting to give you useful information on coronavirus, these apps enable the crooks to access all the information on the device – and even hold you to ransom.

Malicious documents

These documents claim to contain coronavirus-related information. Upon opening them you're asked to 'enable editing' and 'enable content.' Doing so installs malicious software onto your computer.

Practical steps to minimize risk

In the current situation, many people are lowering their guard to phishing attacks and scams. We're more anxious, more eager for information, and therefore less likely to question something that could be suspect.

With that in mind, here are three practical steps you can take to minimize the risk from coronavirus-related attacks.

Enable Multi-Factor Authentication (MFA)

MFA is a great form of defense against attacks that use a fake login page to trick people into entering their credentials.

Raise awareness of these scams amongst your employees

A simple, but effective, step is to always looks at the actual email address used to send the email, not just the display name. (If you're on a mobile device click on the display name to reveal the real email address.)

Sophos Phish Threat, our phishing simulation and training tool, is available to everyone for free for 30 days, and now includes a coronavirus phishing template to help train your teams.

IRS issues warning about Coronavirus-related scams

WASHINGTON — The Internal Revenue Service urged taxpayers to be on the lookout for a surge of calls and email phishing attempts about the Coronavirus, or COVID-19. These contacts can lead to tax-related fraud and identity theft.

"We urge people to take extra care during this period. The IRS isn't going to call you asking to verify or provide your financial information so you can get an economic impact payment or your refund faster," said IRS Commissioner Chuck Rettig. "That also applies to surprise emails that appear to be coming from the IRS. Remember, don't open them or click on attachments or links. Go to IRS.gov for the most up-to-date information."

Taxpayers should watch not only for emails but text messages, websites and social media attempts that request money or personal information.

"History has shown that criminals take every opportunity to perpetrate a fraud on unsuspecting victims, especially when a group of people is vulnerable or in a state of need," said IRS Criminal Investigation Chief Don Fort. "While you are waiting to hear about your economic impact payment, criminals are working hard to trick you into getting their hands on it. The IRS Criminal Investigation Division is working hard to find these scammers and shut them down, but in the meantime, we ask people to remain vigilant."