Coronavirus Phishing Emails

March 2020

Contents

Background to Coronavirus Phishing Emails

Criminals are using the coronavirus to try and bait people into clicking suspicious links in a bid to hack into their computers and steal personal information.

Multiple phishing campaigns have emerged in the wake of the devastating outbreak.

Criminals are claiming to be officials from healthcare groups such as The Centers for Disease Control (CDC), the World Health Organization (WHO) and the National Health Service (NHS).

They purport to offer guidance and information on the COVID-19 outbreak but instead attempt to insert malware and harvest the credentials of unsuspecting users.

How to avoid falling for the Phish

Avoid any inbound emails on this topic **completely** and instead go to "known good" sources of information like World Health Organization (www.who.int), the Centers for Disease Control (cdc.gov) and the National Health Service (NHS) as well as local government and news agencies for any information regarding this situation.

Bad actors are preying on fear; the best strategy is to ignore them completely and follow our spam and phishing guidance.

Example Phishing Emails

Some emails have been seen to state the only way to minimise risk of infection is by avoiding high-risk areas that are listed on a page.

They provide a hyperlink to 'this' page in the email however the link takes the user to sites being run by hackers.

Many emails have been seen that appear to look genuine fooling users into believe they have originated from an @cdc.gov email address therefore making them appear trustworthy.

Emails to date have been seen which:

- Steal user credentials;
- Place malware locally onto machines including key loggers to start tracking all keys entered;
- Have word documents attached that once launched run malicious code to start sending documents from connected drives to criminals.

Examples include: