# 5 Types of Email Threats
## Exploiting Coronavirus Fears

1

### Malware

A number of common malware types are being distributed through coronavirus-related phishing. The first malware reported utilizing coronavirus was Emotet, a popular banking Trojan. LokiBot is another modular malware, which often aims to steal login credentials and data and has been distributed in at least two different coronavirus-related phishing campaigns.

2

### Scamming

Fifty-four percent of COVID-19-related spear phishing attacks were scams. Most of them appear to be offering coronavirus cures and face masks for sale, requesting donations to fake charities, or asking for investments in fake companies that claim to be developing vaccines.

3

### Brand Impersonation

Attacks impersonating well-known brands and services make up around 34 percent of COVID-19 spearphishing attacks. Notably there are a number of attacks impersonating the World Health Organization. These phishing emails appear to come from WHO with information on COVID-19. They often use domain spoofingtactics to trick users into thinking these messages are legitimate. These email impersonation attacks include a link in the body of the email. Users who click on that link are taken to a newly registered phishing website.

4

### Blackmail

Some attackers use raw emotional leverage to get readers to respond out of fear or embarrassment. With heightened anxiety and fear around COVID-19, it's not surprising that some are using that emotion in blackmail or extortion attempts. For example, some attacks have threatened to infect victims and their families with coronavirus unless a ransom was paid—and they make credible claims to knowing who you are, where you live, etc.

5

### Business Email Compromise (BEC)

BEC attacks usually impersonate a person of authority within an organization in order to access funds or valuable information. So far, COVID-19-related BEC attacks make up around one percent of spear-phishing attacks, but their number is growing fast—encouraged by the large number of employees working remotely. These attacks tend to ask urgently for fast payments related to COVID-19, or fraudulently advise of changes to payment methods in order to steal funds.