What to Know About Coronavirus Cybersecurity Scams

Even though the coronavirus (officially known as COVID-19) is proving to be a notable threat, it is precisely these types of incidents that can evolve into a cybersecurity threat.

In the wake of reported deaths related to coronavirus in the United States, there are cybercriminals looking to capitalize on the public fear and urgency surrounding the virus in order to steal personal information and money.

In early February, it was reported that cyber thieves were sending phishing emails related to the coronavirus.

The emails, in this case, are made to look like they are from the Centers for Disease Control (CDC) or World Health Organization (WHO), using domains that are similar to theirs so that the sender appears legitimate.

The email contains an action-inducing subject line that urges the user to open it, such as "Coronavirus Emergency in Your City." The body of the email will sometimes contain stolen logos from the CDC or WHO to make it appear official and will contain legitimate information about the virus.

The most common email attacks prompt users to click on a link to find out more about the virus or to see a list of new cases in their area. This link, though, will take users to a fake website where scammers attempt to collect personal information. The cybercriminals then harvest Microsoft Outlook login credentials, which puts both individuals and businesses at risk. By gaining access to someone's email, the attackers collect any information within Outlook so that they can directly or indirectly gain access to funds.

Another email tactic being used is the placement of malware through attachments or links. Attackers will convince users to open an attachement, and then place malware on the computer, which will compromise the information held on that machine and others within the network.

How to Protect Yourself from Phishing Attacks

Here are some helpful tips to protect yourself from coronavirus related scams:

- The best thing you can do for yourself and those you work with is to educate and inform. Let those around you know that there is a phishing attack going around and not to open or click on anything that looks suspicious.
- Never give another entity login credentials to your email provider. This is personal and private information that should never be shared.
- Check URLs before clicking on them. Some might be misspelled, revealing that they are fake. Even hovering over the link will show that the link does not take you to the desired website, and the email should be deleted.
- If you come across a phishing email, report it to either your IT department at work or the entity it is claiming to represent. Making the CDC or WHO aware of a phishing attempt will help prevent further attacks.
- Do not open attachments from senders you do not recognize or do not typically receive emails from. This is how malware can be transported onto your machine. Instead, reach out to that person and confirm they sent you something. While inconvenient, this one action can potentially save you a lot of trouble in the long run.

If you want to stay up-to-date and informed about the coronavirus, visit the CDC's website to ensure that you receive the most accurate and credible information.

To learn more about how to recognize and avoid phishing attacks, check out the Federal Trade Commission Consumer Information page about phishing scams, located here: **https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing.**