Emerging Coronavirus Scams and Zoom Bombing

(Published on April 3, 2020)*

As the global pandemic continues, coronavirus (COVID-19) scams are also ramping up. We recently are seeing scams where cybercriminals send a phishing email that looks like it is coming from the World Health Organization with important information on the virus. While these scams are still rampant, new scams are emerging that we all must be aware of.

New novel coronavirus scams:

- Beware of interactive maps you find online or on social media. Cybercriminals are circulating a global map of total Coronavirus related cases and deaths. The Map is interactive and accurate with valid current information but the real threat lays in the background. In order to open the map, it must be downloaded by the user – BUT downloading the map will install a keylogger that can steal passwords and information. The map will still function normally, and the user may not be aware they are infected, increasing the likelihood that the map gets shared with friends and family. These malicious maps aren't being used by just one cybercriminal either. The toolkit to run this scam is available for sale on the Dark Web for just a few hundred dollars. There are real and safe interactive maps out there with helpful information, so just make sure you are finding these tools from an accurate and trustworthy source.

- Don't fall for investment opportunities or get rich quick scams related to the Coronavirus. Many scammers are peddling fake companies on the verge of a breakthrough cure or vaccine and need funding to reach their goal. They promise a quick and lucrative profit for those who invest but your financing will only line the pocket of a scammer. Continue to watch out for phishing emails or fake websites playing off these Coronavirus fears. Common scams include teases of vaccines, at home remedies or local health agencies with "important information" about the virus in your community. For the details, the recipient is directed to download an attached file or click on a link. Don't take the bait. Before you click or open anything, know who is sending you the information and what you are being directed to open.

- Phone scams are also on the rise with this outbreak. Over the phone scammers can pretend to be anyone. Their options are endless but as with any suspicious phone call, never give out any sensitive personal information or financial information.

- The healthcare industry is especially vulnerable during this time, as cybercriminals have recognized the intense amount of pressure these businesses are under. Cybercriminals are sending a phishing emails with a word document attached, encouraging healthcare employees to download the attachment which contains "infection-prevention measures". Scammers are also posing as trusted businesses claiming to have personal protective equipment like gloves,

facemasks, and gowns readily available, all of which are in short supply. Some scams have even been reported where individuals are being contacted by a scammer posing as a medical professional, claiming to need personal or payment information to treat their infected family member.

- As we take precautions to safeguard or personal health, lets also apply similar precautions against scammers. Beware of these current emerging scams and inform you friends and family to help protect them as well.

Zoom Bombing

Lastly, as we are all practicing social distancing and tuning into virtual meetings, ZOOM, the very popular virtual meeting tool keeps getting hacked. It's actually called Zoom Bombing. Hackers gain access to a Zoom meeting and attempt to disrupt the video chat and upset participants by shouting profanity or racial slurs, or putting disturbing or offensive images in their video feed. The vulnerability also has people wondering if Zoom is safe to use. Particularly in a large meeting, an unwelcome participant might go unnoticed, enabling that person to record the meeting or otherwise gather information. In particularly sensitive cases, this could become a method of corporate espionage or blackmail.

A couple of quick tips to prevent Zoom Bombing:

- Do not share meeting links publicly. Rather than posting a meeting link to a Facebook group or in a promotional tweet, distribute information via a more private method, such as email.
- Set your meetings to "private." Zoom now sets all new meetings to "private" by default, requiring attendees to provide a password for access. But users often opt to make meetings public for the sake of convenience. Also, the idea of requiring a password is probably worthwhile in keeping your meeting safe.
- Don't use your personal meeting ID. Every registered Zoom user has a personal meeting ID, linked to what is essentially a permanent virtual meeting room. Because that ID doesn't change, sharing it publicly increases the chance that future meetings using your personal ID might be Zoom bombed.
- Share your personal meeting ID only with your most trusted contacts. Generally, while Zoom will prompt you to use your personal ID for "instant" meetings, scheduled meetings will use a one-time meeting ID, reducing risk. If you're concerned that you may have already shared your personal meeting ID in an insecure way, you can contact Zoom directly to have it changed.

This information was provided by navitend

navitend.com
23 US Highway 206 Byram Township, NJ 07874
973.448.0070