MILLER CANFIELD

Cyber-Attacks On The Rise: COVID-19 Scams to Watch Out For

March 26, 2020

As the COVID-19 pandemic unfolds, we are witnessing countless stories of courageous men and women rising up to face the challenges and obstacles of this crisis. Unfortunately, crisis also presents opportunity for unscrupulous individuals to take on less-noble pursuits. During the ongoing pandemic, businesses and individuals should be wary of social engineering cyber-attacks designed to exploit confusion and anxiety in this especially stressful time. The following examples illustrate some of the scams deployed in the wake of the COVID-19 pandemic:

- Phishing "clickbait" emails and social media posts that appear to come from the CDC, WHO, or other well-known organizations seeking donations or offering information;
- Bogus websites providing "free" coronavirus vaccines, treatments, or at-home test kits for a modest shipping fee;
- Targeted emails threatening to infect individuals and their families with coronavirus unless they pay a ransom;
- "Money mule" schemes that take advantage of people who are laid off or sheltered in place by laundering money under the cover of a work-from-home job offer;
- An Android app purporting to provide real-time infection statistics by allegedly scanning a user's location for infected individuals (the app actually turns into an extortion and ransomware tool once the user grants it access to various administrative controls on the device);
- Lastly, and perhaps most bizarrely, ZoomBombing – a phenomenon that involves trolls joining legitimate web meetings and sharing explicit, disgusting, or otherwise offensive content.

The best practices for guarding against these kinds of attacks aren't necessarily new or novel, but they are worth repeating. Be wary of things that seem too good to be true. Don't click on links in unexpected emails or open attachments before verifying the source. Do research before making donations online. Don't be afraid to pick up the phone and call friends, relatives, or colleagues if you receive an unexpected communication asking for an unusual favor. Alert your organization's IT department or the appropriate authorities to potential attacks. Be particularly careful when using personal devices to access work networks. And keep web meetings private or restrict attendees' sharing abilities.

This is part of a series of Miller Canfield **COVID-19 alerts** providing clients with practical advice on measures they can take to navigate through these challenging times. For more legal advice and support, contact Miller Canfield's Cybersecurity and Data Privacy Team or any of the authors of this alert.

This information is based on the facts and guidance available at the time of publication, and may be subject to change.