June 26, 2020

Duke's IT security offices continue to see an increase in cyber attacks related to COVID-19 and are encouraging Duke faculty, staff and students to use caution with all communications including phone calls, email, text and social media. Attackers will try to take advantage of fear about the situation and may use the guise of COVID-19 news to phishing for personal or financial information.

Recent scams include:

- **Antibody testing:** Scammers are marketing fraudulent and/or unapproved COVID-19 antibody tests, potentially providing false results, according to a recent FBI warning [2].
- **COVID-19 research:** The FBI has issued a warning that U.S. health care and research institutions working on COVID-19 response are being targeted by Chinese attackers seeking to obtain intellectual property and data related to vaccines, treatments and testing. Watch this video [3] from Duke's IT security offices. Researchers should be report any suspicious activity to security@duke.edu [4] and should take necessary steps to protect their systems, according to the FBI statement [5].
- **Charity scams:** Organizations or individuals that you don’t recognize may ask for donations in the wake of COVID-19.
- **Online shopping scams:** Cybercriminals may try to sell bogus vaccination or home-testing kits.
- **Email impersonation:** Beware of emails and social media that appear to come from the World Health Organization, the CDC and other reputable sources. If you’re looking for information, visit trusted sites such as the CDC [6], World Health Organization [7], Federal Trade Commission [8] and the Better Business Bureau [9].
- **Robocalls:** Scammers are using illegal robocalls to pitch everything from low-priced health insurance to work-at-home schemes. Calls may appear to come from government organizations [10], family members [11] in distress or banks/credit card companies [12]. Robocalls can be hard to detect since the caller ID can be adjusted to make it look like the call is coming from your area code.
- **Remote work and financial scams:** As more employees are working remotely, attackers are incorporating references to commonly used collaboration tools [13] such as Microsoft Teams and Zoom or using news about financial relief to phishing for personal financial information. More information on coronavirus-related scams can be found on the FBI website [14] and the FTC website [8].
Duke’s IT security offices remind you:

- Don’t respond to texts, emails or calls that seem suspicious. Ignore online offers for vaccinations, and be wary of ads for test kits.
- Hang up on robocalls.
- Watch for emails claiming to be from the CDC or WHO, and don’t click on links from sources you don’t know. Use sites like coronavirus.gov [15], https://www.nc.gov/covid19 [16] and https://coronavirus.duke.edu/ [17] to get the latest information.

If you receive a phone call, email or other communication regarding COVID-19 that seems suspicious, please contact security@duke.edu [4].

A brief video about COVID-19 scams, developed by Proofpoint, is available online [18].

Source URL: https://security.duke.edu/news-alerts/remain-vigilant-latest-scams

Links
[3] https://warwire.duke.edu/w/uckDAA/
[4] mailto:security@duke.edu
[16] https://www.nc.gov/covid19
[17] https://coronavirus.duke.edu/
[18] https://share.vidyard.com/watch/5WfaXCJyoqBwvQCC682d2y?