@DeldigiKNOW

DigiKnow
CYBER SECURITY DEPENDS ON YOU

May 2020

LIVING AND WORKING IN THE TIME OF COVID-19

The Online War Surrounding COVID-19

The Federal Trade Commission has reported more than 22,000 coronavirus scam complaints from all 50 states. ***Please read this newsletter!*** It's important that we protect ourselves against the scammers using the pandemic to steal money and information.

The annual "StateScoop 50 Awards" celebrate the outstanding achievements of our peers and acknowledge their tireless efforts to make a positive impact in the government IT community and in public service. I am honored to be included in this class of extraordinary leaders. **Your vote is appreciated**!!

— **Solomon Adote**, *Chief Security Officer*

Scams and More Coronavirus Scams

COVID-19 and related stimulus scams started in January and continue. The majority are phishing campaigns centered on stimulus payments, fake loans, and other identity thefts. **The IRS won't contact you by phone, email, text message, or social media with information about your stimulus payment, or ask you for your Social Security number, bank account, or government benefits debit card account number.**

Google has detected more than 12 state-sponsored hacking groups using the coronavirus to craft phishing emails in an attempt to distribute malware. One scam targeted US government employees through their personal email accounts with phishing messages posing as coronavirus-related offers from fast-food chains.

Another example is phishing attacks by websites posing as Netflix. Most sites were registered in recent months, including domains that use the virus's official name given by the World Health Organization (example: netflixcovid19s.com).

Be extra cautious with the following:

- Websites with "corona"/"covid" in its domain.
- Files with "Corona"- related file names.
- Email with coronavirus-related subject

Lights, Camera, Videoconference Action!

Working from home, staying at home, checking on family and friends, we're using live video platforms like never before. Zoom has become the platform of choice: Daily participants on the platform surged from 10 million in December to 200 million in March, according to CNET. Zoom's popularity and ease of use has introduced risks that are affecting many users. Recent attacks called "Zoombombing" (uninvited attendees breaking into and disrupting meetings with hate-filled or pornographic content), have impacted critical business, education and public service meetings. Read on for tips on how to use these services more safely and securely. Some content courtesy of CNET.

1. **Selecting the right Video Conference service**: Some video conference solutions are delivered locked-down by design for security purposes (WebEx, Microsoft Teams), others are open by design to enhance the user experience (Zoom). For confidential meetings, the locked down solutions are recommended, when available.
2. **Password protect your meeting**: Set a unique password and where possible a unique meeting ID for all scheduled web meetings. Do not post the meeting passwords to public web sites or in public communication forums. If the meeting is a public one, require registration before providing access.
3. **Enable the "Waiting Room" feature** so that you see who is attempting to join the meeting before allowing them access. Like many other privacy functions, a skillful disrupter can sometimes bypass this control, but it puts another hurdle in their route to chaos.
4. **Disable or control other options, such as Join Before Host** (it should be disabled by default, but check to be sure). Also, restrict screen sharing, file transfers and autosave on chat messages. Most video conferencing solutions provide a settings icon; which looks like a wheel, to make these changes and provide help option to assist in performing these tasks.
5. Once the meeting begins and everyone is in, **lock the meeting** to outsiders and assign at least two meeting co-hosts. The co-hosts will be able to help control the situation in case anyone bypasses your efforts and gets into the meeting.

Questions, comments or topic suggestions? Email us at eSecurity@delaware.gov

DEPARTMENT OF TECHNOLOGY & INFORMATION
DELIVERING TECHNOLOGY THAT INNOVATES

Delaware Department of Technology and Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, or want to print a PDF copy, go to https://digiknow.dti.delaware.gov.