DigiKnow
CYBER SECURITY DEPENDS ON YOU

Contact Tracing and Other Scam Alerts

2020 Info Security Training is Brand New!

We are pleased to bring you the world's leading security awareness training solution, ***KnowBe4*** — a fresh take on delivering this year's mandatory Information Security Training. Engaging and thought provoking, it's aligned to the cybersecurity challenges we face today. **Completing your training takes less than 40 minutes!** Take the training online at your computer (inside or outside State network), either all at once or in several sittings.

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

Federal Trade Commission Issues Alert

Contact Tracing plays a vital role in helping to stop the spread of COVID-19. But scammers, pretending to be contact tracers and taking advantage of how some processes work, are also sending text messages. But theirs are spam test messages that ask you to click a link.

Don't take the bait. Clicking on the link will download software onto your device, giving scammers access to your personal and financial information. Ignore and delete these scam messages.

There are several ways you can filter unwanted text messages or stop them before they reach you:

- Check your phone for an option to filter and block messages from unknown senders or spam.
- Your wireless provider also may have a tool or service that lets you block texts messages.
- Some call-blocking apps also let you block unwanted text messages.

***Contact Tracers in Delaware currently are NOT contacting anyone electronically, only by telephone or personal visit.**

If you have more questions about Contact Tracing in Delaware, call the **Division of Public Health Call Center** at 1-866-408-1899.

Summer's Here. Don't Get Phish-ed!

Beware of Fake Tech Support. Recently a state government employee was contacted by someone pretending to be a legitimate Service Desk/Tech Support person. Unfortunately, this was a phishing attempt and the bad actor was able to temporarily install suspect material on a state laptop. Fortunately, the employee immediately reported the incident, and it was taken care of before any damage could be done.

The Federal Trade Commission (FTC) offers tips on how tech support scammers want to fool you. Their goals include: tricking you into installing malware and viruses, divulging your personal information, or getting you to pay for services you don't need to fix problems that don't exist. To avoid falling for phishing:

- **Never give control of your computer or your credit card** to anyone who calls you out of the blue.
- Security pop-up warnings from real tech companies will **never** ask you to call a phone number. If you see a pop-up urgently insisting that you call, **it's a scam.**
- ***If you are in state government and think there may be a problem with your computer, contact your Service Desk/Help Desk and/or your organization's Information Security Officer (ISO).***
- **Always enable automatic updates and/or update your computer's security software yourself** (or used a trusted tech support company YOU hire) and run your own security scan. Get help and talk with someone you know and trust. Many software companies and Internet providers offer support online or by phone.

Check out this video to see How to Avoid a Tech Support Scam.

And if you get a tech support scam call, block the caller, tell your friends and neighbors about it, then report it to the FTC.

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

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.