Monthly Cybersecurity Newsletter

June 2020
Issue

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

FBI Warning: Cyber Criminals Using COVID-19 to Target Teleworkers

The COVID-19 pandemic has led to an increase in employee teleworking and businesses sharing more information over the internet.

The FBI warns that scammers have seized on the increased teleworking environment and the uncertainty surrounding the pandemic. They have targeted employees of companies by sending fake termination phishing emails and fake video teleconference meeting invitations.

As of April, the FBI has learned that employees from a data security firm received fraudulent emails suggesting the company was terminating employees.

Messages included vague, attention-grabbing subject lines such as "Termination Review Meeting." The emails cited the COVID-19 pandemic as the reason for company downsizing. They gave instructions on how to process out of the company, directing employees to click on a hyperlink in the emails to receive termination benefits. The emails contained a spoofed domain address. Employees who clicked on the malicious hyperlink received a black screen.

In another instance, an FBI investigation determined that attackers had sent email notifications asking employees to join a video teleconference concerning their terminations. The emails contained a hyperlink to a fake teleconference service login page that read "Join This Live Meeting." This helped make the emails appear legitimate. Recipients who fell victim to this attack had their login credentials and other data that was stored on the video teleconference platform compromised.

Businesses and organizations should be on the lookout for the following:

- Calls from employees who mistakenly believe themselves to be terminated

Reporting Cybercrime

State Agencies should report cybersecurity incidents to the ESRMO by contacting the DIT Customer Support Center at (800) 722-3946 or via the incident reporting website at https://it.nc.gov/cybersecurity-situation-report.

Businesses should report suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or at CyWatch@fbi.gov.

Individuals should report such incidents to the FBI at 800-CALL FBI (800-225-5324).

NCDIT Resources

- Avoiding COVID-19 Scams
- Cybersecurity & Working Remotely
- Teleconference Security Tips

- Employees reporting malware or ransomware attacks on their computers
- Employees reporting suspicious activity on legitimate accounts
- Emergence of fake video teleconference applications installed on users' smartphones or computers

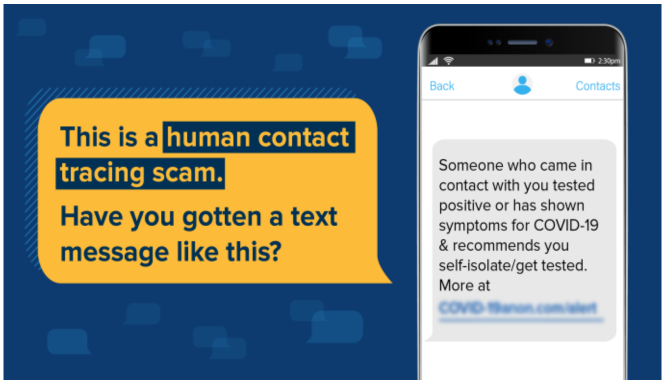
The FBI recommends that employers:

- Alert employees to look for emails coming from Human Resources or management with spoofed email domains
- Select trusted and reputable telework software vendors and be careful when selecting foreign-sourced vendors
- Require the use of a password or PIN for teleconferences or web meetings
- Beware of social engineering tactics aimed at revealing sensitive information. Use tools that block suspected phishing emails or that allow users to quarantine them
- Beware of advertisements or emails purporting to be from telework software vendors
- Always verify web address of legitimate websites or manually type them into the browser
- Do not share links to remote meetings, conference calls or virtual classrooms on open websites or open social media profiles
- Avoid opening attachments or clicking on links in emails from senders you don't recognize

COVID-19 Contact Tracing Text Messages Could Be Scams

Cybercriminals have found a new way to take advantage of the COVID-19 pandemic: contact tracing.

Contact tracing is the process of identifying people who have been in contact with someone who tested positive for a virus, such as COVID-19, and instructing them to quarantine themselves while monitoring their symptoms.


This is a human contact tracing scam.
Have you gotten a text message like this?
Back
Contacts

Someone who came in contact with you tested positive or has shown symptoms for COVID-19 & recommends you self-isolate/get tested. More at

An example of COVID-19 contact tracing text messaging scam. Legitimate messages won't contain weblinks.

In a recent blog post, Colleen Tressler, a consumer education specialist with the Federal Trade Commission, wrote that scammers pretending to be contact tracers are sending text messages to individuals with hyperlinks that if clicked, download malware to the user's device and give cybercriminals access to personal and financial information.

Ignore and delete these scam messages.

Tressler writes that text messages from public health departments are legitimate but they will be limited to simply letting users know to expect a call from a contact tracer.

Read the full blog for ways to filter unwanted texts as well as other steps you may take to protect yourself from scammers.

Scammers Exploit COVID-19: Contact Tracing Scams – What to Watch Out For

Cybercriminals never rest, and they always take advantage of a national crisis to try to trick others into giving them their personal information. They prey on fears while pretending to be tracing the virus. We must remain vigilant and aware of these criminals and their tricks.

Click here to watch a two minute video on NBC Channel 4 in Ohio on how scammers are exploiting COVID-19 contact tracing efforts and how you can protect yourself.

Click here for tips on how to stay secure while working from home.

CYBERSECURITY NEWSLETTERS

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. ***Note**: You must have a valid state employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2020

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS).

- https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute.

- https://www.sans.org/security-awareness-training/ouch-newsletter

Jun 9: Webinar – COVID-19 Cybersecurity Attacks Match the Outbreak Curve

Jun 17: Webinar – Catch and Release: Phishing Techniques for the Good Guys

Jun 19: Webinar – Leveraging Organizational Change to Build a Strong Security Culture

Jun 23: Webinar – Secure Your Data, Your Recovery and Your Mission

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember… Stop. Think. Connect.*