Legislative Council Staff
Nonpartisan Services for Colorado's Legislature

Memorandum

Room 029 State Capitol, Denver, CO 80203-1784
Phone: (303) 866-3521 • Fax: (303) 866-3855
lcs.ga@state.co.us • leg.colorado.gov/lcs

April 8, 2020

TO: Interested Persons

FROM: Andrea Denka, Research Analyst, 303-866-4781

SUBJECT: COVID-19 Cybersecurity Concerns

Summary

As the situation regarding coronavirus (COVID-19) rapidly changes, unique cyber risks are emerging for government, businesses, and individuals. This memorandum provides an overview of cybersecurity, the current threat landscape as a result of COVID-19, and provides information about COVID-19 cybersecurity resources.

Cybersecurity

According to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use. Cybersecurity is needed to protect against cyber threats, which are malicious acts by a person that seek to damage data, steal information, or disrupt a digital function.

According to the Federal Trade Commission (FTC), there are four categories of common cyber threats, which include:

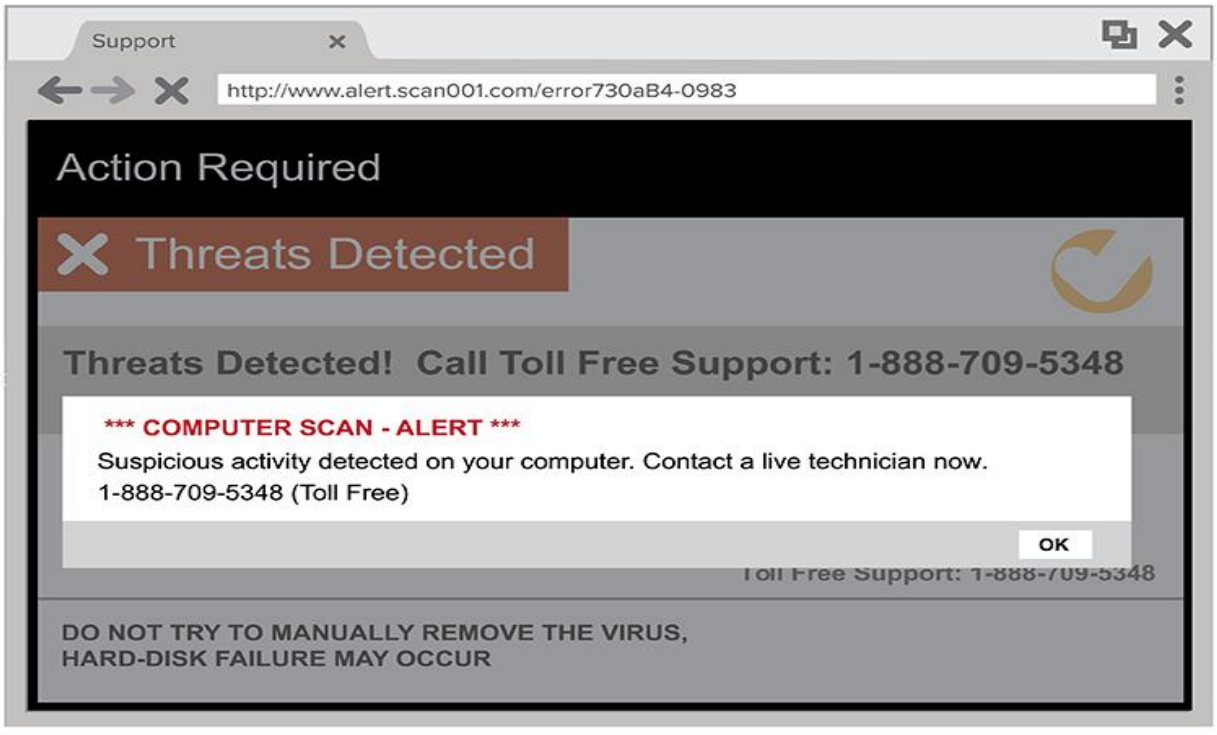
- data breaches, such as the unauthorized acquisition of easily decipherable sensitive or personally identifiable information (PII);
- security incidents, such as an accidental or deliberate event that may cause the compromise or disruption of information technology (IT) systems or intellectual property;
- privacy violations, such as the unauthorized use or disclosure of PII; and
- phishing, which is an attempt to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in an email, telephone call, text (smishing), or on a website.

Cyber criminals are motivated by financial gains, disrupting essential services and functions, and engaging in espionage. Cybersecurity incidents can be unintentional or intentional, and threats can be external criminal activity or people internal to an organization. Example incidents include:

- a disgruntled employee who wishes to cause damage;
- a hacker accessing and damaging sensitive data;
- an organized criminal facilitating social engineering schemes, such as spam emails to obtain PII for identify theft; and
- a terrorist organization breaking into an electrical grid to damage a country's economy.

While cyber threats can target large entities like governments, educational institutions, and businesses, sometimes attackers also gain access through individuals unintentionally giving criminals access. Many cyber attackers create and use robotic calls, emails with malicious links and attachments, and popups with false information to attempt to gain personal information about an individual or an entity. Image 1 is an example of a deceptive scam where the user is asked to call a telephone number for an illegitimate technical support representative, who may attempt to steal PII or financial information to allegedly fix the computer. This scam is often referred to as a tech support scam and can take many forms including the image below or as audio voice announcements.

Image 1
Example of a Cyber Attack



Source: Federal Trade Commission.

Since different types of cyber security threats exist, mitigating security risks can be accomplished in a variety of ways. The FTC explains that the public and private sector use multiple layers of different

technical defenses to protect systems and data, such as installing virus protection, employing IT security staff, and providing employee training. The FTC also provides tips for individuals. Recommendations include: establishing a secure connection to the internet, especially when accessing personal or financial data online; using complex passwords on personal devices and websites; and deleting suspicious emails to prevent clicking on that email's potentially dangerous links or attachments.

Current Threat Landscape

While cybersecurity is necessary for all online activities, the FTC states that cyber attackers are increasingly taking advantage of the fear surrounding the uncertainty of COVID-19 and the growing information available online. Since the onset of the COVID-19 pandemic, the FTC has reported an increase in complaints about robotic telephone calls and emails. On March 9, 2020, the U.S. Food and Drug Administration and the FTC issued warnings that multiple organizations were selling fraudulent COVID-19 products.[1] Reported incidents related to COVID-19 also include solicitations for donations to fake organizations and websites that impersonate government organizations and contain false information.

Besides individuals reporting COVID-19 cyber attacks, many public and private sector organizations are also being targeted as they adopt work-from-home policies. While most cyber threats related to COVID-19 aim to target and harm individuals, larger entities are also experiencing more attacks possibly due to hackers attempting to take advantage of employees working remotely and more people relying on personal internet connections, virtual private networks (VPN), and email communications. For example, the World Health Organization (WHO) reported that cyber criminals set up a fake internal email system mimicking an authentic WHO system in an attempt to steal WHO staff passwords. The WHO released information about increased cybersecurity measures that are being taken to prevent future attacks, including other WHO scams circulating online.[2]

Attempts to gain authorized access to utilities has also been increasing since COVID-19. Utilities are concerned about cyber threats targeting unusual places as electricity usage volumes are changing locations because demand may become higher at private residences. Additionally, the Edison Electric Institute states that cyber threats have increased since the beginning of the year possibly due to the decrease in operators at critical sites, which can cause utilities to be more vulnerable to attacks.[3]

[1] "Coronavirus Update: FDA and FTC Warn Seven Companies Selling Fraudulent Products that Claim to Treat or Prevent COVID-19", Food and Drug Administration: https://www.fda.gov/news-events/press-announcements/coronavirus-update-fda-and-ftc-warn-seven-companies-selling-fraudulent-products-claim-treat-or
[2] "Cyber security", World Health Organization: https://www.who.int/about/communications/cyber-security
[3] "Utilities on high alert as phishing attempts, cyber probing spike related to coronavirus", Utility Dive: https://www.utilitydive.com/news/utilities-on-high-alert-as-phishing-attempts-cyber-probing-spike-related-t/573698/

COVID-19 Cybersecurity Resources

Several organizations have released information about how governments, businesses, educational institutions, and individuals can protect themselves in response to COVID-19.

The Office of the Colorado Attorney General. The Office of the Colorado Attorney General has published several recommendations to avoid potential COVID-19 scams, including deleting any emails from unknown sources about COVID-19, researching any websites that ask for donations to ensure their legitimacy, and staying informed about COVID-19 updates through official government websites like the Centers for Disease Control and Prevention website and the Colorado Department of Public Health and Environment website. More information about potential COVID-19 scams can be found here: https://coag.gov/app/uploads/2020/03/COVID-19_-Coronavirus-Scams.pdf

CISA. CISA has released numerous alerts about COVID-19 scams and the importance of securing critical infrastructure, such as preparing and responding to attacks on utilities. CISA also provides information about how to adopt heightened cybersecurity measures while teleworking. CISA's COVID-19 cybersecurity recommendations, including securing systems while teleworking, can be found on its website here: https://www.cisa.gov/coronavirus

The Federal Bureau of Investigation. The Federal Bureau of Investigation (FBI) released a statement warning organizations within the health care industry of increased fraudulent activity with the purchase of COVID-19-related medical equipment online. The FBI published recommendations to avoid scams, such as being aware last-minute price changes, an unexplainable source of goods that are known to be in short supply, and requests for unusual payment terms, such as a supplier requiring proof of payment. More information about COVID-19 health care cyber threats can be found here: https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-health-care-professionals-of-increased-potential-for-fraudulent-sales-of-covid-19-related-medical-equipment.