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

January 25, 2021

TO: Interested Persons

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

SUBJECT: COVID-19 Cybersecurity Overview

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 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 protects 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:

- *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.

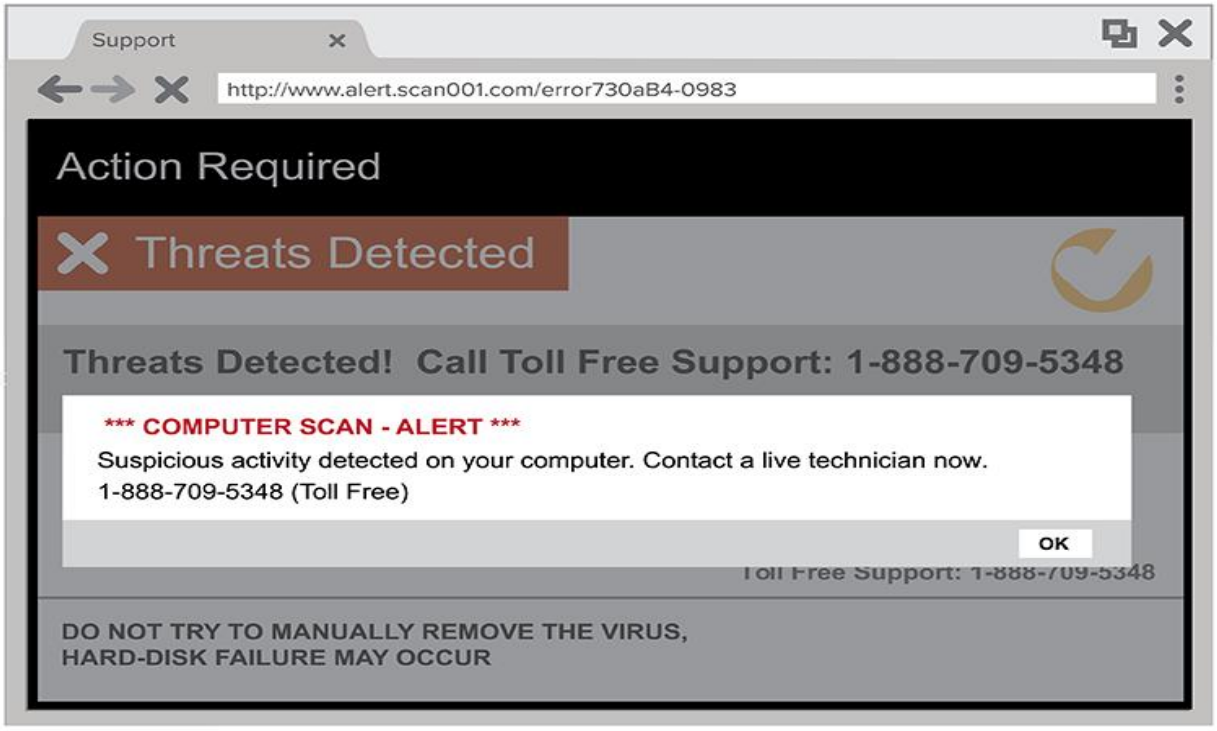
Cyber criminals are motivated by financial gains, disrupting essential services and functions, and engaging in espionage. Threats by external criminal activity or people internal to an organization may be intentional or unintentional. Examples include:

- 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 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. Figure 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.

Figure 1
Example of a Cyber Attack



Source: Federal Trade Commission.

Since different types of cybersecurity threats exist, mitigating security risks can be accomplished in a variety of ways. The FTC recommends 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, cyber attackers are increasingly taking advantage of the fear and uncertainty surrounding COVID-19 and the growing amount of information available online. Since the onset of the COVID-19 pandemic, the FTC noted an increase in complaints about robotic telephone calls, emails, and text messages. The FTC has also released numerous warnings about how people can recognize and protect themselves from fraudulent COVID-19 communications[1]. Individuals have reported incidents such as:

- solicitations for donations to fake organizations;
- links to sign up for vaccinations; and
- emails about accessing stimulus money from the federal government.

Beyond individuals reporting COVID-19-related cyber attacks, many public and private sector organizations are 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) has reported an increase in cyber attacks directed at its staff and internal email system since March 2020. The WHO states that hackers are attempting to target the general public by sending emails through official WHO channels to ask for donations to private funds, which are not associated with the WHO's official COVID-19 fund.[2]

Attempts to gain authorized access to U.S. government data has also been increasing as a result of COVID-19. In December 2020, CISA reported that an international actor was able to gain access into multiple federal government agency networks with monitoring data[3]. U.S. government agencies, critical infrastructure entities, and private sector organizations were targeted in this attack, which is estimated to have started in March 2020. CISA states that this attack allowed hackers to gain classified information on U.S. supply chains, but that as of January 6, 2021, has not disrupted the operations of any targeted organization.

[1]"Coronavirus Resources", Federal Trade Commission: https://www.ftc.gov/coronavirus/resources, last accessed on January 22, 2021.
[2]"WHO reports fivefold increase in cyber attacks, urges vigilance", World Health Organization: https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance, last accessed on January 22, 2021.
[3]"Alert (AA20-352A), Cybersecurity & Infrastructure Security Agency: https://us-cert.cisa.gov/ncas/alerts/aa20-352a, last accessed on January 22, 2021.

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. Recommendations include:

- 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 how to detect fraudulent emails regarding COVID-19 can be found here.

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.

The Federal Bureau of Investigation. The Federal Bureau of Investigation (FBI) released a statement warning individuals about the increase in COVID-19 vaccine scams. These scams include: advertisements to get on a vaccine waiting list, emails offering vaccines for payment, and organizations offering to sell or ship vaccine doses for payment. More information about COVID-19 vaccine scams can be found here.