Addressing Cyber Safety & Security in the Age of COVID-19

Current events highlight the necessity of the "all-hazards, whole-community" approach: a comprehensive effort where plans and efforts address the totality of potential threats – from an attack to a natural disaster, whether a flood or a pandemic.

With respect to the current novel coronavirus (COVID-19), an increasing number of organizations are moving to virtual environments, to include teleworking and Work From Home (WFH) options. This has spurred questions and concerns related to cyber safety as well as security.

CYBER-RELATED ISSUES

At this point in the pandemic, there are three main cyber-related issues:

1. Efforts to compromise systems to disrupt operations or for criminal purposes;
2. Efforts to defraud people, and;
3. Disinformation campaigns.

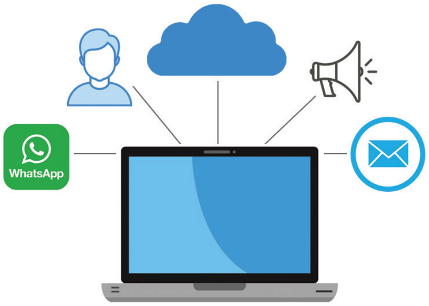
While the opportunity to take proactive measures – assessing one's cyber infrastructure, identifying technical and strategic gaps, and implementing a comprehensive strategy to address them – will have passed for most organizations, both due to the availability of solutions and the time to implement them, there are steps that organizations can take.

IMPACT MITIGATION

At the current time, the best efforts of organizations will be to work to mitigate the potential impacts of an attempted or actual breach. As an organization:

- Organizations should have already tested teleworking solutions
- If available, turn on two-factor authentication on any platforms, software or applications that offer it
- Work with your IT department to ensure all anti-virus software is up to date
- Contact your online donations platform and discuss with them if there are any ways to enhance the security and safety of your efforts
- Re-familiarize employees, staff and leadership on how to identify a phishing scam
- Encourage all team members to take the following actions:
    - Make passwords unique, long and strong
    - Do not use open wifi networks when doing work-related business
    - Be cautious of what you share on social media: cyber criminals often get information through online profiles to increase their chance of success

BASIC PRINCIPLES



There are core principles that are usually covered in a comprehensive planning process, to include the development of Emergency Operations Plans that include annexes for individual man-made and natural disasters or events, such as pandemic. Some of the overarching principles from these plans include:

- Organizations should consider working in the cloud; cloud-based systems should be secure and vetted.
- Do you have updated contact information for everyone?
- Consider back-up communications strategies and plans. Assuming that team members are forwarding their phones, how will organizations get in touch with people if the phone system stops working?
- Think about a redundant email system.
- Have not just a variety of platforms but a plan on when you will use them. For instance, do not just plan to use email or a WhatsApp group or the SCN Alert system. Have a plan for which order you will use them in for team members, so if something happens, they can anticipate an order that you will move through platforms.
- Develop a non-communications plan. What happens, what will people do and how will you organize if you lose all forms of communication?

With respect to disinformation, the release of timely, accurate information and directing people to trusted sources is critical.

To report a cybersecurity threat or incident, please contact:

SCN Duty Desk at 844.SCN.DESK

or email DutyDesk@SecureCommunityNetwork.org