

Cybersecurity and COVID-19

The Hanford Site has rapidly transitioned from normal operations to an essential mission critical operations posture, which also means many employees are now teleworking. While this successful change has allowed our workforce to continue the mission, we need to be aware of the additional cybersecurity risks associated with telework. As information and emails are increasing, scams, hoaxes, and phishing emails are also spreading.

Some examples to be wary of include fake COVID-19 webpages; phishing emails asking for personal information in order to receive a stimulus check; and anyone online seeking to sell products that claim to prevent, treat, diagnose, or cure COVID-19.

We must all be keenly aware of how we protect our sensitive data while teleworking.

Just like social distancing, it is everyone's responsibility to be extra vigilant and consider cybersecurity, especially when teleworking. We need to be sure to avoid the spread of digital disease alongside the pathological one. Please review the attached flyer to find out more information on how to securely perform work from home. As always, report any suspicious emails by clicking the "Report Suspicious Email" button in Outlook or by contacting the Hanford Help Desk at 376-1234. Thank you for protecting the Hanford Site and continuing the mission during this challenging time.



Message provided by



Cyber Distancing

Avoiding the spread of digital disease alongside pathological disease.

Just like social distancing, it is everyone's responsibility to consider cybersecurity, especially when teleworking. Here's what you should do to practice cyber distancing:

1 Limit Travel



Avoid unnecessary or questionable websites. Be especially cautious around COVID-19 related sites, because a number of malicious sites have been created.

2 Stockpile Essential Files

Back up important data on the U drive or network drive, so it can be restored if necessary.

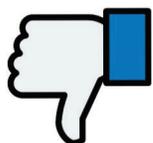


3 Do Not Interact

Be cautious of requests for personal information through emails, texts, and phone calls. Contact the company directly.



4 Distance Yourself



Do not interact with social media sources that may not be reputable.

5 Quarantine Your Sensitive Work



Beware of exposing your sensitive data to other members of your household.

Lock your computer the same way you do when you are at work.



Protect hard copies at home by locking them in a drawer or cabinet.

Make sure that when using Microsoft Teams you are only sharing sensitive information with people who have a need to know. Use a chat session instead of posting in a channel.



Do not send work files to your personal email or store them on your home computer.

Cyber Distancing

Avoiding the spread of digital disease alongside pathological disease.

6 Don't Spread Sensitive Data

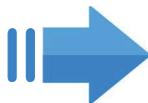
Dispose of sensitive documents by shredding them in an approved shredder, producing strips no larger than one-quarter inch.



Be careful of smart speakers, video doorbells, and other devices that can listen in if you are having a sensitive conversation. Unplug them or relocate them to another location during work hours.

7 Forage for Supplies Safely

With the increase of online shopping, there has been an uptick in web skimming. Web skimming is when a payment page on a website is compromised and malware is injected in order to steal payment information. Be careful where you shop and keep an eye on your transaction history to ensure you don't have fraudulent charges.



8 Be Careful About What You Bring In



Be careful when connecting personal computer peripherals, such as keyboards and mice, to your work computer. Do not connect any peripheral that requires drivers.

Do not plug cell phones into government laptops.



No personal media devices are to be inserted into government devices or used to store government information.

9 Protect Your Router

Your internet router is one of the most important devices in your home and can be prone to exploits by cybercriminals. Make your router more secure by changing your Wi-Fi's default name and password, placing your router in the middle of your home, turning off remote access and more. For step by step instructions visit

<https://heimdalsecurity.com/blog/home-wi-reless-network-security/>