

# 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 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 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.

## 5 Distance Yourself



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

## 6 Don't Spread Sensitive Data

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

## 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.

## 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.

