

The Duh's of Security

Screen/Computer Lock

It's a good habit to lock your computer's desktop every time you leave your computer—no matter how quickly you expect to return.

Although your computer may be set up to lock automatically after a specified time, you should not depend on this function.

It only takes a few seconds for someone else to use your computer while you are away from your desk.

And you'll pay the consequences!



View the video at COVKC.virginia.gov

The Duh's of Security

Eavesdropping

If someone is eavesdropping on your conversation they may be able to obtain sensitive information that could be used to harm you, someone else, or your organization.

When talking about sensitive information, always be aware of your environment and who is around you.



View the video at COVKC.virginia.gov

The Duh's of Security

Local Hard Drive

Saving sensitive information on your computer or mobile device's hard drive, also known as the local drive, is not a secure practice because anyone that uses your computer will be able to access the information, and the information is not automatically backed up.

It is much safer to save the information to network storage drives because they are secured and are backed up regularly.

However, if you must save sensitive information to your hard drive, it must be encrypted and approved.



View the video at COVKC.virginia.gov

The Duh's of Security

Passwords

Your computer's password is the key that unlocks information and related resources for YOUR use. You are responsible for protecting all accessible information as well as any actions taken using your computer account.

You must protect your password from use by other people. There is an even higher risk concerning mobile devices like laptops.

Never put the password directly on the device where it can easily be found—that's just what a thief wants!



View the video at COVKC.virginia.gov

The Duh's of Security

Phishing

Phishing is very much like eavesdropping-
but in electronic form. When you receive
an unexpected electronic message it may be
a trick to get you to disclose personal or
other sensitive information.

Basically they are casting a hook and hoping
you'll take their bait and respond.

Many phishing messages and related sites
not only attempt to get sensitive
information, they may also attempt
to install malicious code,
like a virus, onto your computer.



View the video at COVKC.virginia.gov

The Duh's of Security

Physical Asset Security

Although you have been careful to protect information in the office environment, you must also protect information and devices outside of the office.

Physical asset security includes tangible controls over printed information, laptops, personal digital assistants, and other media devices.

Never leave electronic media where it can be stolen or used without your knowledge.



View the video at COVKC.virginia.gov

The Duh's of Security

Piggybacking or Tailgating

Tailgating, also known as piggybacking, is when a person attempts to enter a secure area or building by following an authorized person.

Use of credentials, like swiping an ID badge, should be used to verify that each person is authorized to enter the area.

Everyone must verify their access, even your fellow co-worker.



View the video at COVKC.virginia.gov

The Duties of Security

Printing

Printed information can be just as sensitive as electronic information and must be handled securely.

Since the printer may not be in your immediate work area, know which printer you are using and pick up sensitive print-outs immediately.

If possible, use a printer that requires entering a PIN-code.

Finally, if the printed version is to be given to someone else, make sure they are authorized to have the information.



View the video at COVKC.virginia.gov