Working Remotely

Technology is enabling more people to work remotely, either from home or while traveling. This provides you tremendous flexibility, but also has certain risks. In this newsletter, we cover some basic steps to help you stay secure.

This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE TECHNOLOGY SOLUTIONS & SERVICES

Working Remotely

Technology is enabling more and more of us to work away from the office, either from home or while on the road. This gives you tremendous flexibility, but also has certain risks. We will show you how you can work both effectively and securely when away from the office.

Working at Home

If you have authorization to work from home, remember that your home network and Internet connection are most likely not as secure as our organization's network. As a result, there are several extra measures you should take to protect yourself and our organization.

While working from home, make sure you only use devices authorized for work. You may not use personal devices, such as personal computers, unless you have management's prior approval. If you have been approved to use personal systems, you may be required to install additional security software. Please check with the help desk or information security team for more information. Also, ensure only authorized people have access to any system used for work. Children, guests or other household members should not have access to your work computer. Unauthorized users can accidently infect your computer or harm the system in other ways.

Protecting Against Loss

While at home or traveling, ensure that any devices you use for work are physically secure. For example, if you must leave your laptop in your car, first secure it in your trunk. If you are using your laptop at a conference all day, consider using a laptop cable lock to secure it. In addition, always double check and be sure you do not forget your devices while traveling. You would be surprised at how many devices are lost simply because someone forgot them. Always be sure to double check that you did not forget your devices when you go through security at the airport, depart a plane, return a car rental or check out of your hotel room.

Connecting Into Work

While working remotely, you may need to connect to our internal networks. Please remember that others can monitor your activities and information when you do so. When you connect from a café, airport terminal or hotel lobby, these public networks can be accessed by anyone and should not be trusted. Any remote connection that will have confidential work information on it should be encrypted. In addition, you may be required to use VPN (Virtual Private Network) software whenever you are connecting to our internal networks or conducting work-related activity. If you are not sure about encryption requirements, please contact the help desk or information security team.

Working Remotely

Securing Your Devices

You will be connecting your laptop or mobile devices to untrusted public networks while traveling. You never know who else is connected to these networks. As such, you need to ensure your devices have been properly secured. Please be sure the following critical protections have been enabled on your devices:

- Ensure your laptop and mobile devices have automatic updating enabled. This ensures they have the latest patches and a current operating system.
- Make sure both your laptop and mobile devices have a passcode or PIN to protect the screen. This way, no one can access them if you accidently lose them.
- Ensure you have anti-virus and a firewall installed and enabled on your laptop.

Using Other Computers

When traveling, be sure you only use your authorized devices for accessing work-related information. Never use publiehese computers are infected. Utilizing them could potentially compromise your login and password.

Losing Your Laptop

There are many threats you have to consider when working remotely. Some examples include cyber attackers who may try to hack your computer and common criminals who want to physically steal your laptop. However, there is another threat you have to consider: yourself. Lost laptops and mobile devices are a common way confidential data is compromised. In many cases, you are more likely to lose a device than have it stolen. When traveling, it is very simple to misplace or forget your mobile devices or laptop. Here are some tips to remember when traveling:

- Always store your laptop and mobile devices in the same bag or location. This way, it is easy to spot if something is missing.
- Make a habit of checking critical items whenever you have passed security checkpoints, left a taxi or exited an airplane.

If you lose a work-related item, be sure to report it immediately.

This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE TECHNOLOGY SOLUTIONS & SERVICES