NWU® | Information Technology

WORKING FROM HOME – PROTOCOL FOR CYBERSECURITY

When working on-campus, NWU IT has put numerous security measures in place to prevent cyberattacks to the NWU network. Working remotely means that staff should put security measures in place at home to secure and protect their Home Wi-Fi-network.

Online threats that remote workers should be aware of:

- **Unsecured Wi-Fi networks:** Most workers will be working from home and they can secure their Wi-Fi. Sometimes unsecured public Wi-Fi networks are used that are prime spots for malicious parties to spy on internet traffic and collect confidential information.
- **Using personal devices and networks:** Many workers will be forced to use personal devices and home networks for work tasks. These will often lack the tools built-in to business networks such as strong antivirus software, customized firewalls, and automatic online backup tools. This increases the risk of malware finding its way onto devices and both personal and work-related information being leaked.
- **Scams targeting remote workers:** We'll likely see an increase in malicious campaigns targeting remote workers. What's more, with many employees lacking remote work opportunities, we'll no doubt see an increase in the prevalence of work-from-home scams.

If you are using your NWU PC or laptop at home during this time, the security settings should be in place. The Wi-Fi network at home must still be secured.

1 Following are some simple steps for staff to secure working remotely:

1.1 Strong passwords.

It's as important as ever to ensure that all accounts are protected with strong passwords. Passwords should be unique for every account, where possible, for example do not use the same basic password for Facebook, your bank account and access to your NWU systems. A password should comprise a long string of upper- and lower-case letters, numbers, and special characters. Use a phrase instead of a word that you can easily remember.

- Never reuse the same password.
- Never share your password with anyone.
- Use a password manager to help you manage all your passwords.

See the following article, http://services.nwu.ac.za/it-news/cyber-security-2-secure-it and select "Strong Password" for detailed information.

1.2 Secure your home router

Your home's wireless router is the **primary entrance for cybercriminals** to access all your connected devices. Secure your Wi-Fi network and your digital devices by changing the factory-set default password and username.

Changing your router password is a good first step, but there are other actions you can take. For example, you should make sure firmware updates are installed so that security vulnerabilities can be patched. The encryption should be set to WPA2 or WPA3. Restrict inbound and outbound traffic, use the highest level of encryption available, and switch off WPS.

1.3 VPN (Virtual Private Network)

This service enables the user who is not on campus to work on the NWU network as if being on campus with access to all services. VPN improves your online privacy and encrypts all your internet traffic, so that it is unreadable to anyone who intercepts it – it keeps information away from cybercriminals.

Note that using a VPN can slow down internet speed. See the IT service catalogue to use VPN: http://services.nwu.ac.za//it/sc/vpn

Read more at: http://services.nwu.ac.za/it-news/cyber-security-3-secure-computing-vpn

1.4 Use an antivirus software

A good antivirus software can detect, and block known malware.

Even if malware does manage to find its way onto your device, antivirus software may be able to detect and, in some cases, remove it.

1.5 Install updates regularly

Updates to device software and other applications are very important. Updates often include patches for security vulnerabilities that have been uncovered since the last version of the software was released.

Make sure your updates are set to run automatically especially outside active hours of work.

1.6 Back up your data

Data can be lost in several ways, including human error, physical damage to hardware, or a cyberattack. Ransomware and other types of malware can wipe entire systems without you having a chance to spot it.

Please backup your data. While hardware backups are still an option, one of the most convenient and cost-effective ways to store your data is in the cloud.

1.7 Beware remote desktop tools

The NWU tool for remote support is AnyDesk. Some of the PC's might still have VNC. Be aware of security problems if you accept an unauthorised remote connection from someone you don't know.

1.8 Look out for phishing emails and sites

Phishing emails, as well as voicemails (vishing) and text messages (smishing) are used by cybercriminals to "phish" for information. This information is usually used in further schemes such as spear phishing campaigns (targeted phishing attacks), credit card fraud, and account takeover fraud.

With the rise in the number of people working from home due to the coronavirus outbreak, no doubt there will be plenty of cybercriminals looking to cash in on the trend. It's highly likely that phishing emails will target remote workers in a bid to steal their personal information or gain access to company accounts.

To spot a phishing email, check the sender's email address for spelling errors and look for poor grammar in the subject line and email body. Hover over links to see the URL and don't click links or attachments unless you trust the sender 100 percent. If in any doubt, contact the alleged sender using a phone number or email address that you find somewhere other than in the suspicious email.

If you do click a link and end up on a legitimate-looking site, be sure to check its credibility before entering any information. Common signs of a phishing site include lack of an HTTPS padlock symbol (although phishing sites increasingly have SSL certificates), misspelled domain names, poor spelling and grammar, lack of an "about" page, and missing contact information.

See the following article: http://services.nwu.ac.za/it-news/cyber-security-4-phishing

1.9 Watch out for work-from-home scams

As well as targeted phishing attacks, we're likely to see an increase in work-from-home scams. Many of these request personal information or upfront payments before you can begin work. By the time you realise it's a scam, the fraudster has ceased contact and stolen your money or taken over accounts.

1.10 Use encrypted communications

Working from home, you still need to communicate with fellow workers, and it's common for those emails to include sensitive information. Groupwise is a secure way of communication.

1.11 Lock your device

If you do have to work in a public space, or if you live with people who you can't share work information with, it's important to keep your device secure. Password-locking your device will usually encrypt its contents until someone enters the password.