Public Advisory: Working Securely from Home

By the end of 2019, South Africa had an estimated 32.6 million Internet users[1], and nearly two-thirds of all households had at least one person who accesses the Internet[2]. The impact of the global novel coronavirus pandemic has greatly increased the number of people working from home. Estimates for August 2020 were that more than half of the country's employees were still working from home[3]. Recent studies indicate that productivity for these employees has not decreased[4], and many companies are expected to continue to allow staff to work from home even after the pandemic is over.

The shift to remote working has many benefits, but also creates new risks for employees and employers, not the least of which are increased security risks. While most companies take precautions to ensure that their office networks are secured against threats, employees working from home may not have the expertise or understanding to do so. The purpose of this advisory is to provide some basic advice that every South African working from home can follow to reduce their security risks.

Five basic security steps

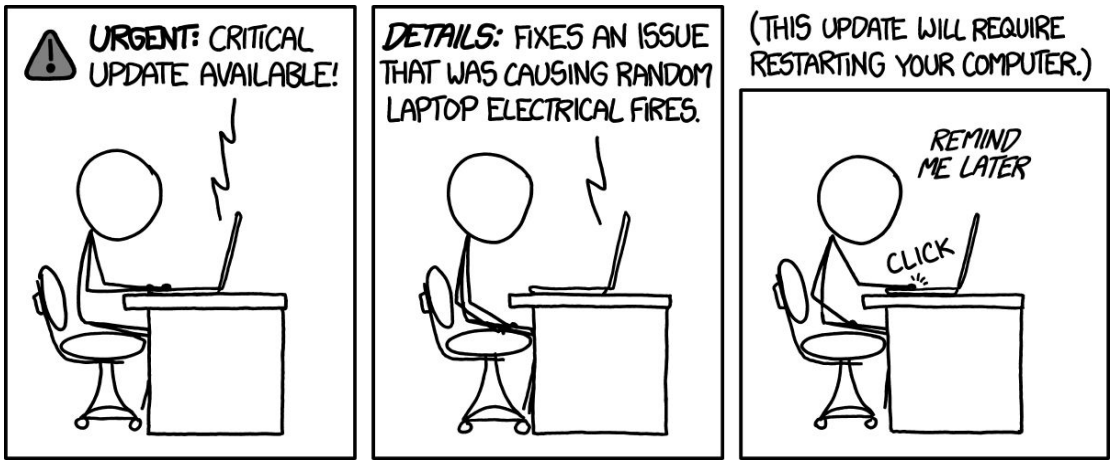
Here are five simple steps you can follow right now to improve your home security.

1. Make sure that you have changed the default password for your wifi router. The default password is not the same password you use when connecting to the wifi, but the administrative password used to log in to your router. Almost all wifi routers ship with a default password, so if you have not changed this, anyone within wifi range can potentially gain access to your router and effectively hijack your home network. For information on changing the administrative password for your particular router, visit the website of the manufacturer. Changing the default password isn't the only way to secure a wifi router. For example, you can also configure the settings so that only specific devices can connect to it based on their unique identifiers (MAC addresses). If you understand how to do that, you should, but if you don't, at least change the default password. Many home offices have more than one router. You may use one to connect to the Internet, and a second (connected to the first) to provide wifi. Make sure you have changed the default passwords for both of them.

2. Backup your data. It goes without saying for everyone, but backups become even more important if you are working from home. Not only does a backup protect you from a physical hard drive failure, but it also protects you against ransomware. This is malicious software that exploits a security vulnerability to seize control of your computer, encrypt your data and then, typically, demand that you pay a certain amount of bitcoin to an anonymous address to regain access to your data. A recent backup eliminates such a threat immediately. Keep your backups in a different location to your computer. If you are backing up to an external drive, unplug that drive and store it in a different room, or even a separate building.

[1] https://www.internetworldstats.com/africa.htm#za
[2] http://www.statssa.gov.za/?page_id=1854&PPN=P0318&SCH=7652
[3] https://www.iol.co.za/business-report/economy/more-than-half-of-employees-are-still-working-from-home-ef21b62c-d5a6-44f1-9f69-a830d6c1fec8
[4] https://yiba.co.za/dramatic-increase-in-remote-working-in-south-africa/

3. Install antivirus software and keep that software and any critical software you use updated. Yes, keeping your software updated can be time-consuming and annoying, but you should do it anyway. Viruses and malware frequently target known vulnerabilities in operating systems and applications, and software updates patch these holes. Antivirus software attempts to identify malicious software before it can do harm, so this adds an extra layer of protection.



Source: https://xkcd.com/1328/

4. Don't use the same passwords for your email and social media. In fact, don't use the same password for anything. Research conducted in 2014 revealed that 54% of people used 5 or fewer passwords for their entire online life[5]. Obviously, this amplifies the damage that can be done if a criminal gains access to one of your passwords. Use a strong password where possible[6]. If you can, use a password manager which can generate strong passwords for you[7]. An increasing number of websites and applications offer two-factor authentication[8]. This combines entering a password with a verification code sent using a different mechanism, for example, to your phone. Where this is available, turn it on. If you are concerned that your password may already have been compromised, there are sites available online[9] which will notify you if your email address has been exposed in a data breach.

5. Be wary of social engineering attacks[10]. That support person calling you from the bank to "verify your personal details" doesn't work for the bank. The lady calling you from a large software company to explain how to "update your computer's security settings" doesn't work for that company. The gentleman calling you to read out the One Time Pin (OTP) sent to your phone to "stop a SIM-swap" doesn't work for your mobile provider. All of them are scam artists trying to gain access to your personal information, your computer or your phone account. None of those companies will ever call you to ask for that information. If in doubt, ask the caller to provide their name and the name of the department of the company they claim to work for and then hang up, Look up the real contact details for the company from a trusted source (e.g. the company's website), and then call the company back. **Never** give out personal information when someone calls you.

[5] https://assets.entrepreneur.com/static/1433198293-password-info.jpg?_ga=1.8425525.1253720500.1466615873
[6] https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/
[7] https://www.cnet.com/how-to/best-password-manager-for-2020/
[8] https://medium.com/@mshelton/two-factor-authentication-for-beginners-b29b0eec07d7
[9] https://haveibeenpwned.com/NotifyMe
[10] A video demonstrating a call centre used for scamming people: https://www.youtube.com/watch?v=le71yVPh4uk

Your computer might be secure, but what about your phone?

For many people, online security is something to worry about on their computer. However, modern smartphones are just as much at risk, and frequently contain a treasure trove of personal information of value to any criminal who gains access to your phone. Here are some basic tips to improve your phone security.

1. Don't install applications you don't need. Delete applications that you don't use. Installing the official app offered by your bank or your mobile provider is likely to be safe. Most mobile app stores also take steps to prevent malicious apps from being added to their stores. However, installing an app from an unknown company can be risky. Even if you trust a company today, and are happy to give their software access to your phone, ownership of the company could quickly change, giving someone new access to your phone and your data.

2. Don't give permissions to applications that don't need them. If that new game your friend is addicted to demands access to all of your phone contacts and all of the pictures you have stored on your phone when you install it, ask yourself: why does it need that? If there isn't a good reason for an app to have access to your data, be suspicious. Either don't install that app, or don't give the app permissions it doesn't need.

3. Backup the data on your phone. This is a good idea for the same reason that it is a good idea to backup the data on your computer. If your phone has a facility to activate a remote wipe of your data in the case the phone gets stolen, make sure you've turned that on and that you know how to use it if you have to. If your phone is stolen, you want to limit the loss to the value of the phone, and not the value of the phone *plus* your personal data.

4. Check the privacy settings for your social media accounts. This is good advice whether you access social media using your phone or your computer, but phone users are less likely to change the default settings. If all of your social media accounts are public, then you are greatly increasing the chances of becoming a victim of identity theft or a social engineering scam. Restrict access to your friends as much as possible. Avoid using your social media accounts to login to other websites, if possible ("sign in using your XXX account"). When you do that, you may be sharing your personal information without realising it.

5. Keep an eye on the data used by your phone. Unexpected data usage can indicate that there is an app sharing information that it shouldn't be sharing. Not only can this be costing you money, but it may also be putting your personal information at risk. Even if your phone is connected to the Internet via a wifi hotspot, so you aren't paying for extra data usage, you should still be wary of any application that is sending an unusual amount of data over the Internet. Check the volumes of data used by your apps on a regular basis.

Securing your email

Email remains by far the most pervasive tool for employees working from home. It is also one of the most common targets for compromise attacks. An email compromise attack occurs when someone impersonates someone else in an email exchange[11]. The purpose of such impersonation is to either gain direct financial benefit or to obtain information that can be used to support further attacks or perform identity theft. The most common form of this attack is via an invoice where the banking details have been changed in favour of the attacker. Often, the invoice will be accompanied by a message that will try and express a need for urgency, in an attempt to circumvent any suspicion or concerns that the intended victim may have.

Here are some steps you can take to reduce your vulnerability to such attacks.

1. Don't click on links in an email if you can avoid it. These links can often be used to harvest your credentials. Similarly, be wary of opening attachments from anyone you don't know. Scammers often hide malware in zipped files with odd file names (e.g. .gz, .tar). If you don't recognise the type of file, the chances are high that it is dangerous. If you get a suspect attachment from someone you know, contact them to query that message before you open anything.

2. Be wary when receiving bank details for a payment online.
    - Scrutinise the sender address carefully. Often a scammer will use an email address that differs slightly from the real address (e.g conpany.co.za instead of company.co.za). Or they may use an address from a free email provider such as gmail.com, or outlook.com.
    - Check if the sender has used the email address before in previous correspondence. If they normally correspond with you via a business email address but are now using a personal email address, that may be because the mail comes from an attacker.
    - Look at the time the email was sent - was it sent after hours or on a weekend? Most businesses will send you invoices during working hours. If the language in the email seems off (grammatical errors, factually incorrect, too much or too little familiarity), that should also be a cause for concern.
    - If the email contains bank details for someone whom you have never paid before or a change of bank details, try and validate these details by phoning the intended recipient. Additionally, many banks allow you to validate the owner of a bank account. There is often a little more work or expense involved with this approach but it is usually worth it.
    - If the email asks for information (ID number, bank account number, etc) that does not seem appropriate for the interaction, try to validate the request by phoning the sender.
    - If in doubt, you can always make a small test payment to the recipient, and ask them to confirm that they received it before transfering the full amount.

[11] A Carte Blanche video covering some South African cases of email compromise: https://www.youtube.com/watch?v=UL5193JSuLM&t=5s

3. Be equally wary of fake bank statements. Scammers will send messages that appear at first glance to be legitimate, but which direct you to entirely fake websites. If you look at the link in a fraudulent message, it doesn't go to your bank's website but sends you to another site instead. These sites look exactly like the real thing but are designed to capture your banking login details. Never click on a link in a mail from your bank, even if you think the mail is legitimate. Instead, open your web browser and type in the website address for your bank. That way, you know you are going to the real website.

4. If you are expecting an email that never arrived or if you never receive a response to an email that you sent, that may be an indication that these emails are being intercepted. If you suspect that this is the case, please contact your company's IT support department for assistance.

5. If your email provider provides you with a web interface to administer your mailbox, check if there are any forwarding or filtering rules that you did not put in place. Filters and forwarding options are usually found under settings. A common method of attack once someone has gained access to your email is to secretly send a copy of your incoming mail to another mailbox or to your spam folder, so the scammer has access to your mail without you knowing.