Tips to avoid inadvertent consumption of your data units and invasion of your privacy

In recent months MTN has received complaints from customers about unauthorized loss of credit from their smartphones. MTN investigations has revealed a number of consumers have applications of which they are unaware running on their phones. These applications, many of which have spyware capabilities, may interfere with phone use and increase data usage. Spyware is any software program that records information about you or what you do on your phone without your knowledge. These spyware could be installed when downloading programs from unsafe sites or attached to free questionable Apps. In other instances it may be pre-installed on your phone by manufacturers in order to track consumer behavior to offer advertisements. There are also dedicated spying apps out there that someone could install on your device if they have access to it for less than a minute. Once you go on the internet on your phone, you'll need to protect your phone. Smartphones are mini computers that need equal protection as your laptop or tablet. That is why we have summarized a number of tips to inform you on how to protect your phone, privacy and your credit.

1. **Beware of installing any third-party software on your device**. This means that the only apps you should use are the ones available through official channels such as the MTN Play, App Store or Google Play. Do NOT download Android apps from unfamiliar sources, even when you use Google play only install applications released by trusted developers that have a good amount of positive feedback.

2. **Always check app permissions when you install the app**. Some applications will ask for personal details and permission to share your information. Be increasingly cautious if an app asks for permissions that seem odd. We advise you stop that installation and avoid the app altogether.

3. **Ensure the settings on your phone are not set to automatic downloads and upgrades of apps** as this could trigger unauthorized downloads particularly in unsecure internet settings. Also we advise that Switch OFF your Bluetooth when not in use. That way, you'll make your phone less vulnerable to cyber attacks and potentially reduce credit loss and a drain on your phone's battery

4. **Set Strong passwords on your phones and tablets** using a combination of symbols, words and figures (e.g. H@l02m#) users of both Android and Apple devices should follow many of the same precautions advised for computer-users. For example, choose strong passwords. (for example, "Password" and "Prince" are not strong passwords.)

5. **Avoid giving out your smartphones to people you don't know** as there are dedicated spying apps out there that someone could install on your device once they have access to it for less than a minute. These apps could make outbound calls or trigger the camera or microphone on your phone remotely.

6. **Get a mobile security app from trustworthy source**s. These can scan apps as you download them to ensure they are clean of viruses and spyware, and continue to check your apps as the mobile threats database gets updated with emerging threats. Reputable mobile security apps will also block dangerous websites that could install malware on your cellphone, and can even scan links sent through text messages. In the event that your device gets stolen, you'll even have the option to block access to your information, or wipe the device completely.

7. More details can be found at http://usa.kaspersky.com/internet-security-center/internet-safety/smartphones or http://usa.kaspersky.com/internet-security-center/internet-safety/cell-phone-spyware

For further information contact MTN Customer Service on 100 or 111