CYBER

Makini Schools

Preschool | Primary | High

KENYA TOP 100 MID-SIZED COMPANIES CLUB 2018/19

UN GLOBAL COMPACT Global Compact Network Kenya

GREAT PLACES TO SCHOOL

UNIVERSITY of CAMBRIDGE International Examinations

ADTECH GROUP

Group IT's CYBERSECURITY

Welcome to Group IT's CYBERSECURITY.
Here is all the information that you need to keep yourself safe when online.
Please remember that your online behaviour can impact our collective IT security which means that we need your help to keep our IT environment safe and running efficiently For any information or questions kindly contact

Cybersecurity@makinischool.com

HOW MUCH DO YOU SPEND ONLINE

Savy South African shoppers are flocking online doubling the size of the online market since 2015 ut risky behaviour online can make you vulnerable

Do's

USE TRUSTED SITES
Stick to reputable sites - Takealot, Amzon or major retailers. Beware of URL misspellings - Crimin al change URL'S to catch you

LOOK FOR THE LOCK
Only buy from the sites that are SSL secured. Look for a locked padlock icon in the address bar and secure URL that includes 's' (HTTPS not HTTP).

SAFE PAYMENT
Don't let sites save your credit card details. Sign up for your bank's OTP (One Time Password). Enable SMS alerts. Check your statements regularly.

USE TRUSTED WIFI
Only use trusted and known public Wifi to shop online. Ensure that your anti-virus (and all other software) is kept updated with the latest version

Don'ts

DON'T OVERSHARE
Give limited personal info online - criminals can do damage with your ID number. Read the Privacy Policy - know how your data will be used.

DON'T OVERSHARE
Use strong/common password, change regularly & never use the same password for multiple accounts. Use a password manager.

INTERNET SAFETY

- The Internet facilitates our inter connected world and make everything from work, shopping, travel and news easier and more accessible. However, there are risks involved in using the Internet and it's important to know how to stay safe online. Check out our campaigns aimed at showing you how to stay safe in an online world

Spot the wolf in Sheep's Clothing

Email impersonation - Where cybercriminals social engineering identity you and then use clever tricks to fool you into thinking that an email has been sent by someone you trust (like your boss) - Is on the rise. If you're not alertt, you could share sensitive information or be defrauded out of money.
So, how do you protect yourself

Be careful what you share online. Criminals identify (& mine info about) targets on social media

If possible, never click on a link in an email. Rather navigate to the site by typing the URL direcly into your browser.

Check email carefully. Small changes to the senders email address or spelling errors in the URL are clues that the email might be a scam

If an email asks for personal info or payment, phone or email the sender separately (using trusted contact) to verify the request.

80%

Rise in Email Attacks over past 12 months

(Mimecast)

R36.5 Million

Cost of Email Impersonation Attacks in 2018

(Ponemon Institute)

Detecting Phishing Email

Don’t Get Hoocked

Unlike spear-phishing/impersonation which targets a specific person, phishing is more a general cybercrime. Criminals target you by email, posing as legitimate institutions (like a bank) to try to lure you into providing sensitive data (like personal info, banking details or passwords). If they get the info, they use it to steal money sensitive information from you.

6 Things to Watch...

Eliminate the Obviouse

Trust your instincts. Check for spelling or formatting errors, look at colours and logos used. Remember that if an email looks fake, it probaly is.

Check Sender’s Address:

Use your coursor to hover over the sender’s address. Idealy, the mailaddress should match the sender’s company/name and country of origin (.co.za).

Consider the source:

Don’t open emails from people that you don’t know. Also, no credible company will ask you to share personal/password info via email.

Be Cautious:

Don’t believe everything you read. Banks won’t alert you to an account breach and heirs aren’t notified of larhe inheritnce via email.

Don’t Click:

Phishing email contain links that, if clicked on take you to fake websites. Attachments (like .exe files) can load malware onto your computer.

BeCheck Signature:

Don’t use the contact information in the signature. Rather, search for company’s contact details on the internet and contact them directly.

Suspect You’re Being Phished?

1 Don’t Reply

2 Alert IT

3 Delete The Email

4 Clear ‘Deleted Items’

EMAIL SAFETY

It’s hard to imagine a world without email! But, like all tech tools that facilitate life and work, email needs to be used responsibly. Check out our campaigns aimed at showing you how to protect yourself from cyber criminals.

MOBILE SAFETY

In our ‘always on’ world, being without a mobile device can feel like torture! But, it’s important to know how to stay safe when using your phone or tablet. Check out our campaigns aimed at showing you how to protect yourself from cyber criminals.

WhatsApp Attack

Recently, attackers exploited a vulnerability in WhatsApp to spread surveillance software to mobile devices trough a phone call. While you can’t check whethe you’re affected, there are the red flags that you can look for...

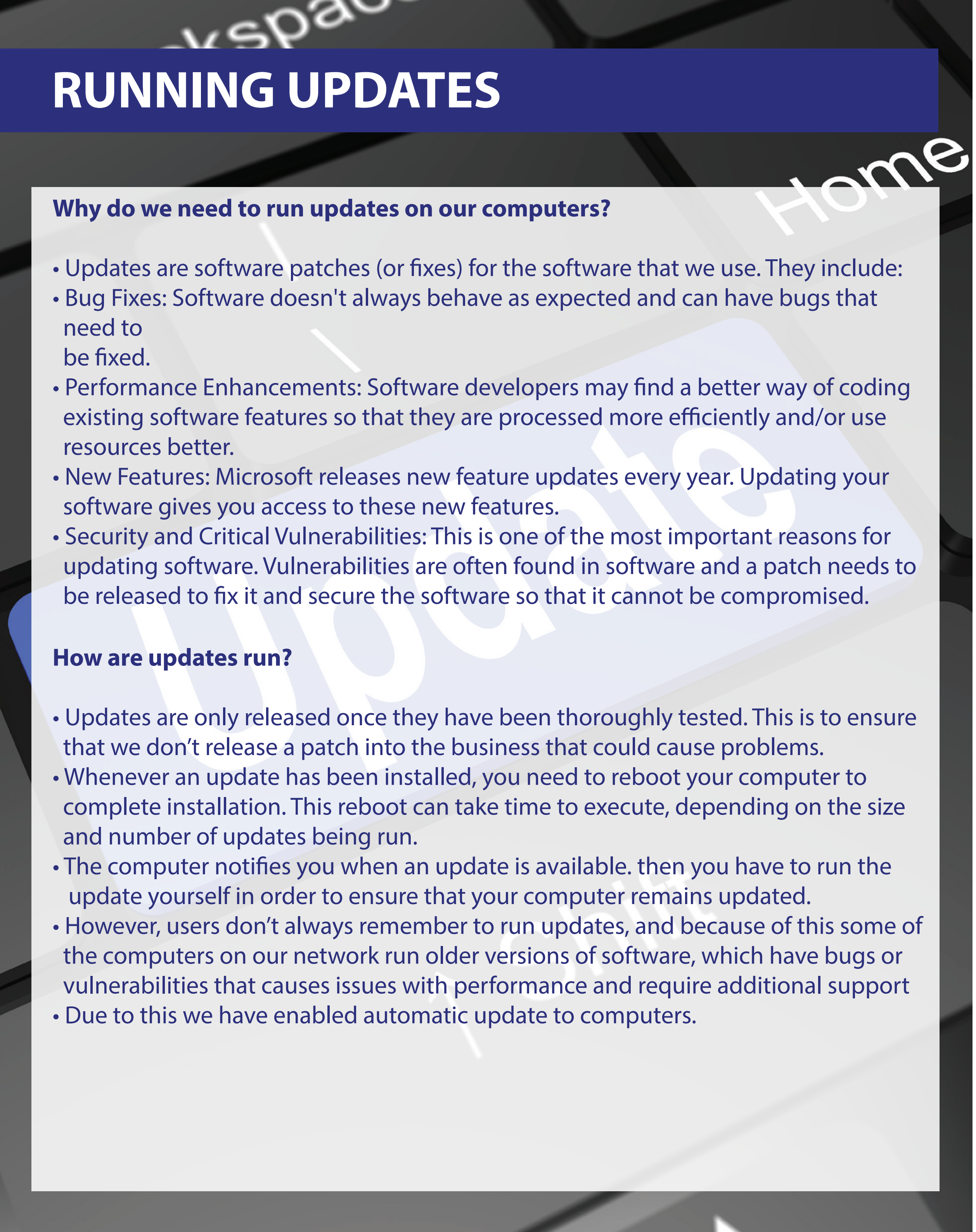
RED FLAGS

Changes in App Usage: Track app usage on yjour device. If an app that you don’t use regularly is using lots of battery life or data, you may have a problem.

Spike in Data Usage: Track your data usage. Spike in data transfers can be a sign that something isn’t right.

What you can do...

Update your device to the **latest version of WhatsApp**
Always **keep** your device’s **mobile operating system up to date** (new OS releases often contain security updates).
Uninstall apps that you don’t regularly use to limit the number of apps that collect your data
.



RUNNING UPDATES

Why do we need to run updates on our computers?

- Updates are software patches (or fixes) for the software that we use. They include:
- Bug Fixes: Software doesn't always behave as expected and can have bugs that need to be fixed.
- Performance Enhancements: Software developers may find a better way of coding existing software features so that they are processed more efficiently and/or use resources better.
- New Features: Microsoft releases new feature updates every year. Updating your software gives you access to these new features.
- Security and Critical Vulnerabilities: This is one of the most important reasons for updating software. Vulnerabilities are often found in software and a patch needs to be released to fix it and secure the software so that it cannot be compromised.

How are updates run?

- Updates are only released once they have been thoroughly tested. This is to ensure that we don't release a patch into the business that could cause problems.
- Whenever an update has been installed, you need to reboot your computer to complete installation. This reboot can take time to execute, depending on the size and number of updates being run.
- The computer notifies you when an update is available. then you have to run the update yourself in order to ensure that your computer remains updated.
- However, users don't always remember to run updates, and because of this some of the computers on our network run older versions of software, which have bugs or vulnerabilities that causes issues with performance and require additional support
- Due to this we have enabled automatic update to computers.

PASSWORD SECURITY

- Having a 'difficult to decode' password is the first step in online safety. Check out our campaigns aimed at showing you how to step up your password security..

FOR YOUR EYES ALONE

NO ONE SHOULD COME CLOSE TO YOUR PASSWORD

Password Security Tips

Passwords should always be a combination of upper and lower case letters, special characters and number.

Consider using a passphrase that is easy to remember and hard to remember to someone else to gues, for example Gold1Lock$-3bears.

Never write your password down or use the same one on multiple sites. Be sure to log out of apps or websites where important passwords are used.
Neveruse your work email account or passwords on social media or 3rd party website.

SPOTTING MALWARE

Malware ('malicious software') is a general term that refers to different types of programs designed to secretly infiltrate your computer and make money off you illicitly, either by stealing, encrypting or deleting your data, hijacking your computer or spying on you without your permission. Malware won't usually damage physical hardware but does threaten your computer safety.

TYPES

SIGNS THAT YOUR COMPUTER MAY BE INFECTED

Ransomware: Your data been encrypted & you need to pay to unlock it.
Browser Redirects: You're redirected to a different site than the one you're trying to reach.
Different Browser Home Page: A different home page appears when you open your browser.
Desktop Icons: New icons appear on your desktop.
Pop Ups: You're bombarded with pop-ups that won't close.
Email: Emails keep bouncing - but you're using the correct address.

SPOTTING MALWARE

BEWARE!

MALWARE ('malicious software') is a general teram that refers to different types of programs designed to secretly infiltrate your computer and make mon ey off you illicity, either by stealing, encrypting or deleting your data, hijacking your computer or spying on you without your permission.

Malware won't usually damage physical hardware - but does threaten your computer saftey.

CAN YOU PREVENT MALWARE INFECTIONS

Think before you **CLICK** on links or attachments.

Run **UPDATES** personal regularity

Don't **OVERSHARE** personal data.

Use **STRONG PASSWORDS**.

BACK UP to OneDrive regularly.

Practice **SAFE BROWSING**. Log out when done.

LIMIT App privileges.

Remove **OLD/ UNUSED** software.

Scan **FLASHDRIVERS** before use.

cybersecurity@makinischool.com

Makini Schools

Preschool | Primary | High

Parental Controls

This helps in giving your child a safe space to explore their curiosity online.

What can Parental Controls do?

Parental control can offer different functions depending on the provider, these include:

- Setting specific time limits on your children's use
- Controlling/Blocking games your child can access
- Prevent children from using specific programs
- Manage content children can search for online

PARENTAL CONTROL FOUND IN DIFFERENT PLAT FORMS.

1. Parental Controls from your Internet Service Provider(ISP)
Setting Parental Controls through your ISP can be the easiest way to manage what your children can access across all your devices and computers at home. This service is free on most ISPs.

2. Parental Controls on your Computer Operating System
Most computer systems offer easy to follow steps on setting up parental controls, which are free to use.

3. Parental Controls on Smartphones and Tablets
Whether your child has access to an Android/Apple smartphone or tablet, parental controls are available across all of these devices. You can turn off functions like in-app purchasing, social networks, app store access, camera access, Bluetooth and more.

4. Parental Controls on your Internet Browser.
Most internet browsers offer free restrictions to help manage what your child can access when online.

5. Parental Controls on Search Engines.
Search engines play a big part in what we look at online so it is important to help manage the types of content your child can come across when searching for something online.

6. Parental Control on Video Sites.
- YouTube: has also recently introduced a free YouTube kid's app, which may also be worth considering for your child.
- Netflix: You can control access to certain maturity levels of Netflix content from the Your Account page under Manage Profiles.

7. Parental Controls on Game Consoles
In many households, gaming can be just as popular as or even more popular than spending time online, so it is just as important to protect our children when gaming. The most popular consoles all offer free parental controls and easy systematic guides to setting them up.

A FEW CONCERNS PARENTS SHOULD TALK ABOUT OR DO TO THEIR CHILDREN.

- Talk with your child about ways to use the internet and cell phones safely.
- Talk with your child about ways to behave toward other people online or on the phone.
- Talk with your child about what she/he or she does on the internet.
- Talk with your child about what kind of things that should not be shared online.
- Check to see what information was available online about your child.
- Check your child's social network site profile.
- Check which websites your child visited.
- Befriend your child on social media.

HOW TO SET PARENTAL CONTALS

Hi Parents,
It is very simple to set up this controls and setting.

Below link is a systematic guide, which will help to make it simple and straightforward for different devices and platforms. You can download or send the instructions after selecting your option.

https://www.internetmatters.org/parental-controls/

IT MAKINI.

Makini Schools

Preschool | Primary | High

Kaspersky Safe Kids

Kaspersky Safe Kids is a multi-platform solution that provides protection for your children. You must have a My Kaspersky account. If you do not have an account, you can create one right away.

You can install Kaspersky Safe Kids by click of the word in blue for Windows, Android, iOS, and Mac devices. After installing the application, you will initially get the free version with a limited number of features. To use all the application's features, activate the premium version with an activation code for Kaspersky Safe Kids or Kaspersky Total Security.

With Kaspersky Safe Kids you can:

- Control the time your child spends on their device.
- Limit the time your child can play games or use social networks.
- Receive detailed reports on your child's online activity.
- Monitor your child's activity on social networks.
- Get information about your child's location and be notified when they leave the allowed area.
- Control the installation of applications.
- Set access rules for websites and applications.
- View information about the battery status of your child's device.

Click "Kaspersky Safe Kids Parental for Portal Tour"

IT TEAM
MAKINI SCHOOL

Makini Schools, Makindi Road, P. O. Box 21784 - 00505, Nairobi
Email: cybersecurity@makinischool.com
www.makinischool.ac.ke