Volume 9 Issue 6: 6th February 2023

Tudor Grange Academy Kingshurst

Sixth Form

Sixth Sense

Which Week?

This Week: Monday 6th Feb (Week 1)

Next Week: Monday 13th Feb (Week 2)

UCAS

Top 5 Student Tips for Those of You Who Have Applied to UCAS

Top 5 tips from UCAS for our Year 13 students who have applied to study at university from September 2023.

1. If you have used all five choices on your applications but are not holding any offers, you may be eligible to use UCAS 'EXTRA' when it opens on 23 February. Link to UCAS Extra.
2. You can make some changes to your application after submission, or you might need to contact the university or college. Link to what you can and cannot change.
3. Once the application has been submitted, you can sign in anytime to track your application and find out about the different offers you may receive and the dates to reply. Link to date information. Link to what 'Clearing' is.
4. Any student who has made Undergraduate and Conservatoire applications can accept offers through both schemes until they receive confirmation decisions. Link to Conservatoire applications.
5. **REMEMBER: It's not too late to apply. Applications can be submitted until 30 June 2023 when they will be entered into Clearing. Speak to Miss Foster and Mr Bowers if you are interested in this.**

Safer Internet Day 2023

Safer Internet Day an international event that is held every February in over 170 different countries. The goal of Safer Internet Day is to call on people across the world to work together to make the internet a safer and better place for all, but especially for young people such as yourselves, and aims to start a national conversation about using technology safely and positively.

This Safer Internet Day asks everyone to make space for conversations about life online, especially with young people, because you have the right to have your say on issues and policies that impact YOU and by doing so, influences decisions that governments, social media and gaming platforms and technology companies make in respect to changing their practices to keep you safe.

Borrowing a Laptop

Just to keep you all updated and prepared, we will be moving towards a system where an ID card will need to be handed-in when borrowing a laptop due them left being left rather than returned. **Please ensure you are equipped with your ID card.**

NOS

Our series of information from National Online Safety, continues on this week with a focus on building a degree of cyber-resilience at home, a place of which where you are likely to interact most with online technology. The outcome of this will reduce the likelihood of any cyber attack gaining access to your account . As ever, clear advice is provided on page 2 of Sixth Sense to enable you to protect yourself electronically to best effect.

For any feedback, please email: (Yr12) Mr Curran: ccurran@kingshurst.tgacademy.org.uk, **(Yr13) Miss Foster:** jfoster@kingshurst.tgacademy.org.uk; **(Learning Mentor) Ms Akhtar:** norakhtar@kingshurst.tgacademy.org.uk, **Mr Bowers:** jbowers@kingshurst.tgacademy.org.uk **(Director of Sixth Form)**

12 Top Tips for BUILDING CYBER RESILIENCE AT HOME

As a society, we're increasingly using technology and tech services in the home. Digital assistants which can adjust the heating or turn lights on and off; streaming services for shows and movies on demand; games consoles; smart speakers; phones; laptops ... the list goes on. As we introduce each new gizmo to our homes, however, we increase the level of threat from cyber criminals. It's essential, therefore, that we learn to become more cyber resilient in relation to the devices and digital services that the people in our household use.

WHAT IS 'CYBER RESILIENCE?'

*Cyber resilience focuses on three key areas: reducing the **likelihood** of a cyber attack gaining access to our accounts, devices or data; reducing the potential **impact** of a cyber incident; and making the **recovery** from a cyber attack easier, should we ever fall victim to one.*

1. PASSWORDS: LONGER AND LESS PREDICTABLE

The longer, less common and predictable a password is, the more difficult it becomes for cyber criminals to crack. The National Cyber Security Centre's 'three random words' guidelines are ideal for creating a long password which is easy to remember but hard to guess.

2. AVOID RE-USING PASSWORDS

When you use the same password across different logins, your cyber resilience is only as strong as the security of the weakest site or service you've signed up for. If cyber criminals gain access your username and password for *one* site or service, they'll definitely try them on others.

3. USE A PASSWORD MANAGER

A good way to juggle different passwords for every site or service you use is to have a password manager. This software stores all your passwords for you, so you simply need to remember the master password. LastPass, Dashlane, 1Password and Keeper are all excellent password managers.

4. BACK UP YOUR DATA

Keep a copy of your data using OneDrive, Google Drive or another reputable cloud-based storage solution. If it's extremely important or sensitive information, you could even decide to keep more than one back-up version – by saving it to a removable USB drive or similar device, for example.

5. ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Multi-factor authentication is where you need access to your phone (to receive a code, for example) or another source to confirm your identity. This makes it far more difficult for cyber criminals to gain entry to your accounts and your data, even if they *do* manage to get your username and password.

6. CHOOSE RECOVERY QUESTIONS WISELY

Some services let you set 'recovery questions' – such as your birthplace or a pet's name – in case you forget your password. Take care not to use information you might have mentioned (or are likely to in future) on social media. More unpredictable answers make cyber criminals' task far harder.

7. SET UP SECONDARY ACCOUNTS

Some services provide the facility to add secondary accounts, phone numbers and so on to help with potentially recovering your account. Make sure you set these up: they will be vital if you're having trouble logging in or if you're trying to take back control of your account after a cyber attack.

8. KEEP HAVING FUN WITH TECH

Consider our tips in relation to the gadgets and online services your household uses. Protect yourself and your family, and don't let the bad guys win: devices are not only integral to modern life but also a lot of fun – so as long as you keep safety and security in mind, don't stop enjoying your tech.

9. CHECK FOR BREACHES

You can check if your personal information has been involved in any known data breaches by entering your email address at www.haveibeenpwned.com (yes, that spelling *is* correct!). It's useful if you're worried about a possible attack – or simply as motivation to review your account security.

10. CHANGE DEFAULT IOT PASSWORDS

Devices from the 'Internet of Things' (IoT), such as 'smart' home appliances, are often supplied with default passwords. This makes them quicker to set up, but also less secure – criminals can identify these standard passwords more easily, so change them on your IoT devices as soon as possible.

11. KEEP HOME DEVICES UPDATED

Download official software updates for your household's mobile phones, laptops, consoles and other internet-enabled devices regularly. Security improvements and fixes are a key feature of these updates – so by ensuring each device is running the latest version, you're making them more secure.

12. STAY SCEPTICAL

Cyber criminals commonly use various methods, including emails, text messages and social media posts. Be cautious of any messages or posts that are out of the ordinary, offer something too good to be true or emphasise urgency – even if they appear to come from someone you know.

Meet Our Expert

Gary Henderson is the Director of IT at a large boarding school in the UK, having previously taught in schools and colleges in Britain and the Middle East. With a particular interest in digital citizenship and cyber security, he believes it is essential that adults and children alike become more aware of the risks associated with technology, as well as the many benefits.

Source: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-word | https://haveibeenpwned.com

National Online Safety®
#WakeUpWednesday