

Head Teacher: Mr D Barrow

Mortimer Road
Kenilworth
Warwickshire
CV8 1FS
01926 854450
www.st-johns.warwickshire.sch.uk

19th October 2017

Dear Parents and Carers,

ONLINE SAFETY – YEAR 3

In our online safety lesson, we have been learning about passwords. We know that we shouldn't tell other people our passwords, except for our trusted adults. We shouldn't use any personal information or nicknames in our password because they are easy to guess. Our password should contain at least eight characters and we should change them every six months. We had a go at making our own passwords using random words.

From 3B, 3T, Miss Baker and Mrs Tennant

Common Sense on Online Security



What's the Issue?

Learning to protect personal identity information, creating strong passwords and being cautious when downloading programmes and files are crucial to children's safety as well as the security of the information stored on their digital devices. Otherwise, children can expose themselves and their families to digital threats such as computer viruses, data and identity theft, and hacking.

To understand digital safety and security, you'll need to learn perhaps some unfamiliar words: phishing, malware, spyware, spam and yes, even junk. These refer to greedy little programmes that attach themselves to respectable-looking software, e.g. a downloadable game that looks really cool and then wreak havoc once installed on our computer.

Why Does It Matter?

If children don't protect their personal information, there are many potential risks: damage to the hardware, identity theft and financial loss. Children may not realise that they are putting their information in jeopardy because the warning signs aren't always obvious. For instance, another child might ask for your child's computer password to play a game and then access your child's private email account. Or your child might use a file-sharing programme that passes along a virus to your computer. Older primary school children might be asked to provide personal identity information such as home phone number, address, or date of birth, by a thief posing as someone else, all of which opens up the family to the risk of identity theft. Just like in real life, children online have to know who to trust with information.

common sense says

Help your child master the fine art of password creation. Teach them:

- **Not to use passwords that are easy to guess, such as their nickname or their pet's name.**
- **Not to use any private identity information in their password.** Identity thieves can use this information to pretend to be them.
- **Not to use a word in the dictionary as a password.** Hackers use programmes that will try every word in the dictionary to guess passwords.
- **To use combinations of letters, numbers and symbols.** These are harder to crack than regular words because there are more combinations to try.

Teach your children to be careful with what they download. Let them know not to download free games or videos to their computer. These programmes often come with spyware and viruses that will land the computer in the repair shop – and them in hot water. In the end, what seemed like free software often comes at a cost.

Let your children know how to identify and deal with spam. Teach them that spam is Internet junk mail. They should not open it because, if they do, they will just receive more of it. The best strategy is not to open email from addresses they don't recognise.

Powerful Passwords

* DID YOU KNOW ...

The most popular password is "123456."
Yikes -- that is NOT a secure password!

Trace each word

community

advertise

product

* WHAT DO YOU THINK?

Why are strong passwords helpful?

1. Family Activity

With a parent, practise creating passwords that are hard to guess and relatively easy to remember. Write down the name of a book, TV show, movie, or something else you like. Then abbreviate the phrase, replace some of the letters with numbers and symbols, and make some letters uppercase and some lowercase. For example, "Clifford the Big Red Dog" could become "Cl1ffB1Grd." What are some ways that you can remember your password?

* DO YOU REMEMBER ...

How to create a secure password?

2. Tech It Up!

Try a child-friendly online-password generator! Go to www.dinopass.com with a parent and see if you can come up with a story to help you remember the password it generates.

3. Common Sense Says ...

Don't make your password something that others can easily guess! Remember not to use a dictionary word or your nickname (since this would be easy for others to guess). Make your password secure by checking that it includes letters, numbers, and symbols. (Hint: !, @, \$, and % are examples of symbols.)