St John's Primary School and Nursery

Warwickshire County Council

Head Teacher: Mr D Barrow

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

21st October 2016

Dear Parents and Carers,

ONLINE SAFETY – 5S

In online safety, we have learned about staying safe online, what to do and what not to do on the internet, and how to ensure our passwords are strong. We also discussed SMART rules with our online safety officers. At home, we are going to make sure we keep safe online and report any disturbing messages or videos we receive. As well as this, we talked about the importance of not deleting messages so that they can be kept as evidence.

This week, we learned how to make sure our passwords are strong. We will make sure they are eight or more characters long and we will ensure we do not include any personal information such as name, birthday or home address. To keep it as strong as possible, we found out that it is best not to use a word from the dictionary, but to make one up instead and to use symbols, capital letters and numbers. We will also change our passwords every six months to make sure that they are safe.

Parents and carers, attached to this letter is some home learning that we (the children) would like you to complete over half term. We will support your understanding and guide you through the process so that you can be as knowledgeable online as we are!

From 5S and Mr Sharp

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.

Strong Passwords

✱ DID YOU KNOW ...

One of the most commonly used passwords is "qwerty," and this is NOT a secure password! (Can you figure out why so many people might use this password? Hint: Try typing it out on a computer keyboard.)

Unjumble to find the hidden words

1. srteiucy _____
2. etatopecxin _____
3. bolbhaipirgy _____
4. pawrossd ptriooectn _____
5. rodnam _____
6. seecrn nmae _____

✱ WHAT DO YOU THINK?

How can we remind ourselves, other students, and our families to keep passwords secure?

✱ DO YOU REMEMBER ...

How a secure password helps you protect your private information?

1. Family Activity

With a family member, review the Common Sense dos and don'ts of creating a safe password. Then, pick your favourite cartoon character and draw a picture of him or her on a piece of paper. On the back of the paper, make a list of personal information (interests, fun facts) about the character and use it to make up a safe and secure password for your character. Check that you haven't included any PRIVATE information -- only use personal information. Next, try to come up with a story to remember the password.

2. Tech It Up!

DinoPass (http://www.dinopass.com/) is a password generator for kids that has two options: SIMPLE passwords and STRONG passwords. Try generating at least three of each and write them down. With a family member, see if you can spot a pattern to figure out the difference between the STRONG and the SIMPLE passwords. Together, come up with at least one pro and one con of using each type of password.

3. Common Sense Says ...

Smart and safe passwords: 1). have at least eight characters; 2). use a combination of letters, numbers, and symbols; and 3). aren't easy for other people to guess! Passwords should NOT have private information in them, such as your full name (first and last), date of birth, mother's maiden name, street address, school name or address, credit card number, phone number, or social security number.