

**National Support School**

designated by



National College for  
Teaching & Leadership

Mortimer Road

Kenilworth

CV8 1FS

01926 854450

[www.st-johns.warwickshire.sch.uk](http://www.st-johns.warwickshire.sch.uk)

**Head Teacher: Mr D Barrow**

8<sup>th</sup> February 2018

Dear Parents and Carers,

## **ONLINE SAFETY – YEAR 5**

On Safer Internet Day (6<sup>th</sup> February 2018) and in our online safety lessons this half-term, we have been looking at spam (the junk mail, not the food). We discussed what spam actually is, and how it is similar to some kinds of letters that you do not want and did not ask for. We talked about the different kinds of spam: advertising, false advertising, fake prizes and offers of money, and emails that look like they are from your bank but are really an attempt to steal your personal information. We then looked at some scenarios involving children who had been the victims of spam, and thought about what might happen next and what they could have done differently. We learnt a lot about this online safety danger and how we can stay safe and vigilant in the future!

**From 5C, 5S, Miss Cooke 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.

# You've Won a Prize!

## \* DID YOU KNOW ...

According to the government's CAN-SPAM Act, businesses are required to let people stop getting emails from them. That means you should always see a way to "unsubscribe" from an email listserv, which is something businesses use to send the same email to A LOT of people at the same time.

## Match the words to their definition

password protection	something that a company advertises and sells
computer virus	the requirement that visitors use a password when they access a website so that only certain people can view the site and participate in its online activities
citation	key information about a source used for a report or other research project, including its author, title, publisher, and date of publication
product	a software program that can damage other programs on the computer

## \* WHAT DO YOU THINK?

What is the safe thing to do if you get an email or IM from a stranger?

## \* DO YOU REMEMBER ...

What spam is and what you can do about it?

## 1. Family Activity

With a parent or family member, create a poster about how to identify and deal with spam. Design the posters for kids who are two years younger than you and who likely do not know anything about spam. Ask your family members what they do when they receive spam, and consider adding their tips to your poster. If you have a computer at home, put your poster up near the computer to remind everyone what to do with spam.

## 2. Tech It Up!

Use Glogster ([www.glogster.com](http://www.glogster.com)) to make a digital version of your poster.

## 3. Common Sense Says ...

Spammers want you to open their emails. Follow these spam-stopping tips -- don't fall for tricks!

- Don't open messages from people you don't know.
- If you open a message by mistake, don't click on links or download files that come with it.
- Never reply to emails or IMs from people you don't know.
- Don't reply to spam, even to tell the spammer not to send any more messages.
- Flag emails as "junk" or "spam."
- Watch out for messages that ask for your private information. No one should ever do this.
- Tell an adult you trust about any message that makes you uncomfortable or that comes from someone you don't know.