

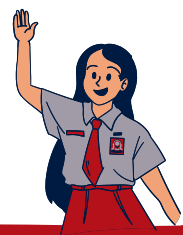
# SCAMMING & INTERNET FRAUD

EVERYTHING YOU NEED TO KNOW....

**Scamming is an extremely serious problem!**  
Today's cybercriminals are more creative than ever in finding ways to worm into computers and bank accounts around the world.



**A scam is an illegal scheme aimed to steal from others, and unfortunately, people of all ages and backgrounds are targets for these crimes.**



The people behind these scams try to trick people into giving away their money, personal or financial details, and the scary thing is, it is becoming more and more difficult to figure out what's real and what's not!



**Scams come in a lot of different ways – emails, text messages, phone calls, websites etc.**



## **WATCH OUT FOR THE FOLLOWING WAYS....**

### **ACCOMMODATION SCAMS**

When you finally get some time off work and are planning to jet away with your friends, you obviously need somewhere to stay! But be careful!! **Accommodation scams are everywhere**, and these criminals will try to rent you a lovely spot by the beach that may not even exist!



### **CHARITY SCAMS**

Another common method of draining people of their money is by **impersonating a charity or a cause**. Scams in the common day are ruthless, it is so important to double check everything before handing over money or personal details!



### **"SMISHING" SCAMS**

**Ever heard of smishing?** This is a term used to describe when scammers use fake text messages to trick people to download dodgy software, share sensitive information or click on a link to hack the victim's phone – triple-check that any messages sent to your phone are legitimate!



### **SOCIAL MEDIA SCAMS**

The people we follow on Instagram, Twitter etc. might not be who we think they are! Only follow people you know, as scams through **false endorsement** and links are becoming a scary issue



# BE WARE OF....

- Watch out for **unknown contacts** from a person or company out of the blue – for example, with banks – ALWAYS contact your bank before clicking on a message from them. Generally, banks don't send messages, so be careful!
- Have you come across **a deal that seems too good to be true?** That's because more often than not, it is! If there is pressure to enter personal details or respond quickly, this brand or person is not to be trusted!
- **Misspelling** – this is an easy way to indicate whether or not you are faced with a scam – automated messages that are misspelled are rarely from high profile companies – be weary!

**IF YOU HAVE BEEN SCAMMED, YOU MAY BE ABLE TO GET YOUR MONEY BACK, CONTACT YOUR BANK AND SEE WHAT THEY CAN DO.**



**AND MOST IMPORTANTLY....REMEMBER THAT IF YOU HAVE BEEN SCAMMED, IT CAN HAPPEN TO ANYONE, SO FEEL NO SHAME OR EMBARRASSMENT! THE WAY THESE SCAMS ARE CREATED NOWADAYS, IT'S ALMOST IMPOSSIBLE TO FIGURE OUT WHAT'S GENUINE.**