Villa Real School
together we achieve

# Online Safety at Villa Real School Autumn 2024 Newsletter

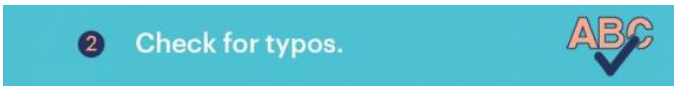
## Phishing attacks


Everyone is susceptible to a phishing attack. Often, phishing emails are well-crafted and take a trained eye to spot the genuine from the fake.


Email addresses and domain names can be easily spoofed. It is crucial that you check the domain name for spelling alterations on suspicious emails. Even if they appear to have come from a trusted sender, always double check.

**multimedia.com**
**multirnedia.com**

Can you tell the difference between these two addresses? (The 2nd one is fake!)



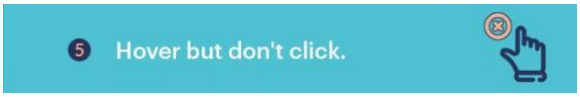

Attackers are often less concerned about being grammatically correct. Which means that typos and spelling errors are often evident in messages. Such errors in an email could be a good indication that the message is not genuine.


Any email that asks for sensitive information about you or is suspicious. For instance, no bank will ever ask for personal information over an email. Directly call your bank to find out if an email is genuine or not.

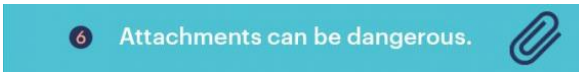

Phishing attacks use scare tactics such as urgency and authority to trick victims into taking immediate action. Emails that ask to share personal information or to make cash transactions are... 'phishy'.

Villa Real School
together we achieve

# Online Safety at Villa Real School Autumn 2024 Newsletter



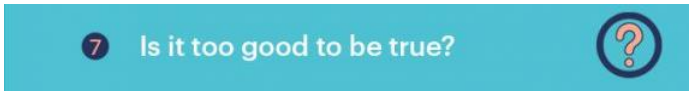

Hover over URLs. If the alt text does not match the display text, or if it seems strange, DO NOT click on it. To ensure you don't fall for schemes like this, you must train yourself to check where links go before opening them. Thankfully, this is straightforward: on a computer; hover your mouse over the link, and the destination address appears in a small bar along the bottom of the browser. On a mobile device, hold down on the link, and a pop-up will appear containing the link.



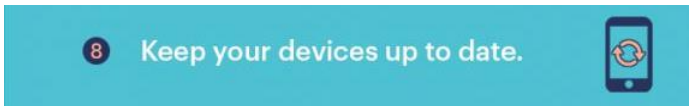

Hover over attachments to check for an actual link, before you click on it or download it. But, if you are still unsure of the sender, do not click on the link.

';--have i been pwned?

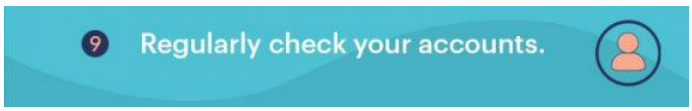
https://haveibeenpwned.com/




If it sounds too good to be true, chances are it is! Phishing attacks use fake rewards to tempt victims to take action. You wouldn't win a lottery if you never participated.




Devices, and the applications on them, are more susceptible to attacks when systems are not updated. Maintain your antivirus and regularly check for updates for your operating system.




Check your accounts regularly to ensure that no changes have been made without your knowledge. Staying on top of your accounts, and knowing what data is held in each, will make spotting a phishing attack easier.

'Have I Been Pwned?' is a free service that's worthwhile to find out if your email address has been compromised, which could then lead scammers to try and contact you with phishing email campaigns. If your email address is listed it may be worth changing it!