

Online Safety Monthly Bulletin

For Parents and Carers

Edition 4

February 2025



Miss Hyland – Computing Coordinator



Safer Internet Day

Every year, Whitehall Junior School joins a nationwide campaign, Safer Internet Day. This year it falls on 11th February.

The theme for this year is: **Too good to be true? Protecting yourself and others from scams online.**

It will be an excellent time to have a discussion with your children about scams they have noticed online. Perhaps even challenge them to let you know whenever they see something they think is a scam.

Children will need to practise identifying threats with:

- offers that are too good to be true
- contact that they didn't expect
- personal information being asked for
- money or trade being asked for

Discuss what your child should do if they are scammed. If children know that they do not need to feel ashamed when an incident happens, they will be more likely to alert a trusted adult.

AI and scamming

The next spam call you receive may not be a real person. Scammers are increasingly using voice-enabled AI models to automate their fraudulent schemes. The human ear was not designed to tell the difference. The tricking of individuals by imitating real human callers, has become a new and highly effective methodology enabled by AI advances.

<https://www.techradar.com/computing/artificial-intelligence/ai-voice-clone-scams>

Contact Us

If you have any concerns or questions regarding online safety or your own child's well-being, please email the Whitehall Junior School office on: office@whitehalljunior.org

Visit our parent [Online Safety](#) webpage for previous Online Safety Bulletins and further information.

This issue...

- Safer internet Day
- Scams

Top Tips

- Set up phones, consoles, tablets and computers with parental control settings.
- Have open and honest conversations with your child about what they are accessing and what is acceptable.
- Guide children to appropriate games and activities.
- Follow age rating guidance.
[Common Sense Media](#)
- Keep up to date with trends through [our newsletter and online safety website page](#).

Helpful Links

CEOP – Child Exploitation and Online Protection



Internet Matters



BOYS

What Parents & Educators Need to Know about QR CODE SCAMS

WHAT ARE THE RISKS?

QR code scams (also known as 'quishing'), involve the malicious use of Quick Response (QR) codes to deceive people into revealing personal information or downloading harmful software. These scams exploit QR codes' convenience and widespread use – for example, in adverts, restaurant menus and public notices, with criminals installing fake QR codes which direct users to bogus sites.

PAYMENT SYSTEMS

Cybercriminals may seek to change a QR code that's related to a legitimate payment service, such as in a restaurant. If a customer scans the QR code expecting to order and pay for goods or services (such as a meal in this case), they may be directed to a site controlled by the scammers. Entering their payment details would then allow the criminals to defraud them.

DISCOUNTED GOODS

A poster promises goods or services at a discounted cost, requiring people to scan a QR code to register and pay. The poster, however, is malicious, and there is no discount. Again, providing your payment details would allow the criminal to access your funds. This scam is reasonably common and is often found in car parks in major cities.

PRIZE DRAWS

A QR code is provided for a prize draw, advertised on a poster which is likely on display in a public space. Scanning the QR code will result in being asked to provide further information (such as your email address, name, address or phone number), which is then used by criminals for further social engineering attacks or even identity fraud.

WIFI CONNECTION

Scanning a QR code may be the means of connecting to the Wi-Fi network in a hotel or other public area. This is usually legitimate, but if the QR code is a fake, it could result in criminals viewing your browsing history and even your login details. These can subsequently be used for phishing attacks and identity fraud – and even financial fraud, if they're able to access your banking credentials.

FAKE EVENTS AND TICKETS

A poster highlights news regarding an upcoming event, or regarding an additional allocation of tickets for a sold-out concert or other performance. It directs the user to scan a QR code for more information, to register or possibly to pay. The QR code then leads to a fake site hosted by scammers, aiming to gather data on the user for future attacks or to exploit or defraud them immediately.

Advice for Parents & Educators

BE VIGILANT

QR codes are becoming more prevalent, and cyber criminals are increasingly seeking to use them to steal information and commit fraud. As such, it is important to remain aware of the risks. Always consider these safety concerns before scanning a QR code and avoid doing so unless you're certain it's legitimate. Be sure to keep your device's operating system updated as well, to keep you protected from known safety risks.

CHECK FOR SIGNS OF TAMPERING

Where QR codes are printed or displayed, check for any sign of tampering: as a sticker with a new QR code being placed over the top of the previous code, for instance. Where there are signs of tampering, you should consult a member of staff (if you're in a hotel or restaurant, for example) or simply avoid scanning the code altogether.

CHECK THE URL

Most phones now show the web address or URL which a QR code connects to, and they typically require users to accept being taken to this address before progressing. Check that the web address matches that of the site or service you're expecting to access via the QR code you've scanned. If it seems dubious in any way, don't click on it.

USE TRUSTWORTHY SOURCES

Consider the source of the QR code and its trustworthiness. A QR code for payment in a restaurant, for example, is likely to be legitimate if you can see it printed on every menu; a random poster pinned up in the street or in a building's corridor is more likely to be fraudulent. If you're unsure, err on the side of caution and don't scan the code.

USE THE DEFAULT QR CODE SCANNER

Most mobile devices come with the ability to scan QR codes built into the camera app. Where possible, you should seek to use this default functionality and avoid the use of third-party QR scanning apps which may have themselves been tampered with or compromised. Stick to reputable methods.

Meet Our Expert

Gary Henderson is the Director of IT at Millfield, a large independent boarding school in Somerset, as well as a member of the Digital Futures Group, Vice Chair of the ISC Digital Advisory Group and an Association of Network Managers in Education (ANME) Ambassador.



#WakeUpWednesday

The National College®