NIFC COMMUNITY AWARENESS UPDATE

NIFC COMMUNITY AWARENESS UPDATE 6/22 (13 Jun 22)

(The Community Awareness Update provides general information to enable personnel to keep up-to-date with routine correspondence; it is not provided for mission-related items and does not replace the Emergency Messaging System.)

PROTECT YOUR Pa$$W0RD Campaign: (Courtesy of Neighbourhood Watch.)	If strengthening your passwords is something you keep putting off, or you feel overwhelmed by the sea of online security information, you're not alone. As part of the Neighbourhood Watch Cyberhood Watch initiative, launched in 2019 in partnership with Avast, they are re-running the PROTECT YOUR Pa$$W0Rd campaign that targets both the overwhelmed and complacent, providing everyone with three (3) easy steps to be more secure online. PROTECT YOUR Pa$$W0Rd in 3 easy steps: • Create a separate password for your email account. • Use 3 random words. • Turn on two-factor authentication (2FA).
SMSFactory – Stealth malware: (Courtesy of Neighbourhood Watch.)	A malware campaign targeting Android users across the globe is racking up high phone bills for victims. The stealthy malware strain, named SMSFactory by Avast, infiltrates phones and uses trickery to hide itself on the device so the victim is unaware of the damage being done. Within just one year, Avast has protected more than 165,000 people around the world from this threat. As malware attacks such as SMSFactory become increasingly common and difficult to spot, it's important to know what to look out for and the preventative measure to take. What is SMSFactory? • The malware sneakily taps money from victims by sending premium SMS and making calls to premium-rate phone numbers undetected. One version is also capable of extracting victims' contact lists, spreading the malware further. How does SMSFactory infiltrate a device? • This kind of malware is being spread through malvertising, a type of cyberattack that abuses adverts to send people to websites hosting malware. • SMSFactory also appears to be distributed through push notifications and alerts displayed on sites offering game hacks, adult content, or free video streaming sites. The malware is disguised as an app which people can download. Once installed it hides itself, making it nearly impossible for victims to detect the cause of the additional charges on their phone bills. What masking techniques does SMSFactory use? • SMSFactory uses several tricks to stay on the victim's device and remain undetected. It has a blank icon and it is able to hide its presence by removing its app icon from the home screen. The malware relies on the user forgetting about the app on their phone so they are unaware of the financial damage until they receive their phone bill. Tips on how to avoid mobile malware like SMSFactory:

Is it an emergency? Call 999

If it is <u>not</u> life threatening: Call 101 for the Civil Police; Call 111 for the NHS.

If you want to report a concern anonymously, you can report it via the Crimestoppers website or via their hotline on: 0800 555 111.

NIFC (24/7): 01480 847013

	- Stick to official app stores SMSFactory highlights the importance of using verified app stores to install applications. Third party stores or unknown sources may contain malware and aren't blocked by an authority, such as Google. - Install an antivirus on your mobile device This is especially important if you choose to install apps from unofficial sources. You can also be protected from malicious websites this way. Antivirus software acts as a safety net, protecting even the most careful users. - Remain vigilant It's important to remain cautious when downloading new apps, especially apps advertised in short and catchy videos, or through push notifications in the browser. - Disable or limit premium SMS with your carrier While there are legitimate uses for premium SMS, recent SMS malware campaigns highlight the importance of having control over additional charges on your phone contract. Disabling premium SMS features – or at least setting a limit – significantly limits the potential impact of campaigns like this. This step is especially important on children's phones.
OUNDLE Food Festival – Sat 18 Jun 22:	The annual Oundle Food Festival is back and will be held on Sat 18 Jun 22 (1100-1600). The one day Food & Drink extravaganza welcomes many independent producers and food vendors from the region, and further afield. Well worth a visit but you will need to park on the outskirts – look on it as a walk to the Food Fest to work up an appetite and a walk back to the car to work off the pounds/kilos you have just put on.
Cambs Police – Seatbelt Checks:	A two-week enforcement campaign begins today to ensure everyone is staying safe and wearing their seatbelts. Our officers will be sharing safety messages and looking out for those flouting the rules. Buckle up or face a fine.

Is it an emergency? Call 999

If it is not life threatening: Call 101 for the Civil Police; Call 111 for the NHS.

If you want to report a concern anonymously, you can report it via the Crimestoppers website or via their hotline on: 0800 555 111.

NIFC (24/7): 01480 847013