The Parish of Berrick Salome
Oxfordshire

Chairman: Ian Glyn
Vice-chairman: Ellie Cross
www.berrickandroke.org.uk

Clerk: Chris Cussens
Mokes Corner, Berrick Salome
OX10 6JR
Tel: 01865 891197
parish-clerk@berrickandroke.org.uk

March 14th 2020

Coronavirus covid-19

The Parish Council has considered what its response to the coronavirus covid-19 situation should be.

We see our role as directing parishioners to information and guidance from reputable government sources and encouraging people to continue with normal village life as much as possible within these guidelines.

In this respect the main government website to refer to can be viewed here.

See also NHS 111 Online.

Those of you with access to the internet may also wish to look at the community Facebook group 'Friends & Residents of Berrick, Roke & Rokemarsh', although this is not a parish council group.

One of the merits of living in a close and tight village community is the spirit of friendship and co-operation that exists between friends and neighbours. The council hope that everyone will keep eyes and ears open for those that may require extra assistance.

We also want those who do require such extra assistance to know who to contact and to feel comfortable so doing.

Whilst the situation with coronavirus persists, the PC will make itself available, on an informal basis, to try coordinate the provision of this extra assistance where necessary and in extremis.

If assistance is required please use the Parish Clerk's email address or, if you do not have email facilities, call Ian Glyn on his personal mobile number 07831 635159 or landline 01865 8910041.

The PC will also continue to circulate relevant guidance from the authorities as it is received by us. This will mainly be by email. For those who do not have email or have not provided consent for the PC to use their email address, important information will be hand delivered.

Unfortunately, there are cybercriminals who are exploiting the spread of coronavirus. The NALC (National Association of Local Councils) has issued the information contained in the attached appendix to help prevent you falling into the fraudsters' traps.

Appendix

Cybercriminals exploit the spread of coronavirus
Wednesday, 11 March 2020
Author: Stuart Wilbur, Microshade Vsm

Microshade VSM works in close co-operation with cybersecurity experts to ensure the safety of local (parish and town) councils' data. We wish to share this information with the sector that has given to us.

Since February 2020, the National Fraud Intelligence Bureau (NFIB) has identified 21 reports of fraud where coronavirus was mentioned, with victim losses totalling over £800k. It's expected that reporting numbers will rise as the virus continues to spread across the world.

What are the risks?
The two most common risks are:

- Viruses — These are malicious software programmes loaded onto the user's computer without their knowledge and performs malicious actions, leading to corruption of data/files, or even altogether disabling the computer.
- Phishing — This is the fraudulent attempt to obtain sensitive information such as usernames, passwords and bank details by disguising oneself as a trustworthy entity in an electronic communication.

Of the reported coronavirus related fraud cases, ten of these reports were made by victims that attempted to purchase protective face masks from fraudulent sellers. Fraudsters are also sending out coronavirus-themed phishing emails in an attempt to trick people into opening malicious attachments or revealing sensitive personal and financial details.

Some of the tactics we've identified from victim reports include fraudsters purporting to be from research organisations affiliated with the Centres for Disease Control and Prevention (CDC) and the World Health Organisation (WHO) contacting potential victims over email. They claim to be able to provide the recipient with a list of coronavirus infected people in their area. To access this information, the victim needs to click on a link which takes them to a malicious website or requested to make a payment in Bitcoin.

What should I do next?

- Watch out for scam messages — Don't click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for personal or financial details,
- Protect devices from the latest threats — Always install the latest software and app updates to protect devices from the latest threats. The National Society for Cyber Security provides useful information on **how to update your devices**.
- Shopping online — If you're making a purchase from a company or person you don't know and trust, carry out some research first and ask a friend or colleague for advice before completing the purchase. If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases. Action Fraud, the UK's national reporting centre for fraud and cybercrime, has produced **advice on how to shop online safely**.