CYBER SECURITY POLICY

GENERAL SECURITY POLICY

The Crediton Town Council Cyber Security Policy provides a concise set of security polices enabling the Council to manage the security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent security efforts will be based. They define the appropriate and authorised behaviour for personnel approved to use Crediton Town Council information assets. Appendix One provides a set of procedures for the Council to follow in the event of a Cyber Security Breach.

Applicability

The Crediton Town Council Cyber Security Policy applies to all employees, councillors, contractors, volunteers and anyone using Crediton Town Council information assets. Information assets are defined as any information system (hardware or software), data, networks and components owned or leased by Crediton Town Council or its designated representatives.

General Policies

All employees, councillors, contractors, volunteers and any other person using or accessing information or information systems must adhere to the following policies.

- All information systems within Crediton Town Council are the property of and will be used in compliance with Crediton Town Council policy statements.
- Any personal information placed on Crediton Town Council information system resources becomes the property of Crediton Town Council.
- Any attempt to circumvent Crediton Town Council security policy statements and procedures (ie, disconnecting or tunnelling a protocol through a firewall) is strictly prohibited.
- Unauthorised use, destruction, modification and/or distribution of Crediton Town Council information or information systems is prohibited.
- All users will acknowledge understanding and acceptance by signing the appropriate Crediton Town Council policy statements prior to use of Crediton Town Council information assets and information systems.
- At a minimum, all users will be responsible for understanding and complying with the following policy statements:
  - Cyber Security Policy
  - System Security Policy
  - Desktop Service Security Policy
  - Internet Acceptable Use Policy
  - Personal Equipment Policy
  - Virus, Hostile and Malicious Code Policy
- All users will report any irregularities found in information or information systems to the Town Clerk or Assistant Clerk immediately upon detection.
- Information systems and information will be subject to monitoring at all times. Use of Crediton Town Council information systems constitutes acceptance of this monitoring policy.

- Use of any Crediton Town Council information system or dissemination of information in a manner bringing disrepute, damage or ill-will against Crediton Town Council is not authorised.
- Release of Crediton Town Council information will be in accordance with Crediton Town Council Policy Statements
- Users will not attach their own computer or test equipment to Crediton Town Council computers or networks without prior approval of the Town Clerk.
- If a user fails to comply with this policy, they will face disciplinary proceedings. Penalties can range from a verbal warning to dismissal. The actual penalty applied will reflect the severity of the violation and prior violations.

SYSTEM SECURITY POLICY

Crediton Town Council's System Security Policy addresses access control, use of hardware, operating systems, software, servers and backup requirements for all systems maintained and operated by Crediton Town Council.

Applicability

The System Security Policy applies to all Crediton Town Council employees, councillors, contractors, volunteers and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the Town Clerk.

Password System Security

Crediton Town Council has adopted this policy to ensure that private information and council data is kept secure at all times. Authorised users must comply with creation, usage and storage policies to minimise risk to corporate information assets.

- Passwords will conform to the following criteria:
  - Passwords will be a minimum of seven characters
  - Passwords must consist of at least one uppercase letter, one lowercase letter and one number.
- The sharing of passwords is prohibited.
- Any suspicious queries regarding passwords will be reported to the Town Clerk.
- Passwords will be protected as Crediton Town Council proprietary information. Writing them down or storing them unencrypted on the information system is prohibited.
- Users must change their passwords every 90 days and may not reuse passwords that have been used previously.
- Users will be forced to unlock their computers using their network password after 15 minutes of inactivity on their desktops.
- Users must lock their computers when their desktop is left unattended.
- All system passwords will be changed within 24 hours after a possible compromise.
- When users leave the organisation, their accounts will be immediately disabled or deleted.
- If the user leaving the organisation was a privileged user or a network administrator, all system passwords will be changed immediately.

DESKTOP SERVICES SECURITY POLICY

The Crediton Town Council Desktop Services Security Policy addresses the authorised and legitimate use of hardware, operating systems, software, LAN, file servers and all other peripherals used to access any information system.

- All Crediton Town Council information will be held on the NAS RAID1 Storage Device.
- Three external USB Back-up drives are used, with logs detailing when back-ups are undertaken. Crediton Town Council will check the back-ups to ensure they have been successful and rotate the back-ups weekly.
- Cloud Backup from NAS Device is available.
- No software of any kind will be installed onto a laptop or desktop computer without the approval of the Town Clerk
- Only system administrators will have the ability to install software.
- Unauthorised copying or distributing of copyrighted software is a violation of UK Copyright Law and will not be permitted.
- Personal software will not be installed on any Crediton Town Council machine.
- Users will not allow non-employees to use any Crediton Town Council machine or device without authorisation of the Town Clerk.
- The following items are corporate policy for security monitoring:
  - All Crediton Town Council systems and network activities will be subject to monitoring. Use of Crediton Town Council systems and networks constitutes consent to this monitoring.
  - Disabling or interfering with virus protection software is prohibited.
  - Disabling or interfering with logging, auditing or monitoring software is prohibited.
  - All Crediton Town Council desktop services will be subject to inventory and inspection.
  - Security irregularities, incidents, emergencies and disasters related to Crediton Town Council information or system will be reported to the Town Clerk immediately.
- The following items are council policy for system usage:
  - Sabotage, destruction, misuse or unauthorised repairs are prohibited on Crediton Town Council information systems.
- All repairs will be authorised by the Town Clerk and performed by the Cosmic IT team.
  - Desktop resources will not be used to compromise, harm, destroy or modify any other service or resource on the Crediton Town Council information system.
  - All data on information systems at Crediton Town Council is classified as company proprietary information.
  - Users will secure all printed material and other electronic media associated with their use of Crediton Town Council information and information systems.
  - Storage, development or the unauthorised use of tools that compromise security (such as password crackers or network sniffers) are prohibited.

INTERNET ACCEPTABLE USE POLICY

Internet access is provided to Crediton Town Council employees to conduct Crediton Town Council business. While these resources are to be used primarily for Crediton Town Council business, the council realises that employees may occasionally use them for personal matters and therefore provides access to non-offensive personal sites during non-business hours.

- The definition of non-business sites is the sole discretion of the Town Clerk. This definition can, and will, change without notice as the internet continues to evolve.
- Internet activity will be monitored for misuse.
- Internet activities that can be attributed to a Crediton Town Council domain address (such as posting to newsgroups, use of chat facilities and participation in email lists) must not bring disrepute to Crediton Town Council or associate Crediton Town Council with controversial issues (ie, sexually explicit materials).
- Internet use must not have a negative effect on Crediton Town Council operations.
- Users will not make unauthorised purchases or business commitments through the internet.
- Internet services will not be used for personal gain.
- Internet users will make full attribution of sources for materials collected from the internet. Plagiarism or violation of copyright is prohibited.
- Release of Crediton Town Council proprietary information to the internet (ie, posting information to a newsgroup) is prohibited.
- All internet users will immediately notify the Town Clerk of any suspicious activity.
- All remote access to the Crediton Town Council internal network through the internet will be encrypted and authenticated in a manner authorised by the Town Clerk.

EMAIL SECURITY POLICY

The Crediton Town Council Email Security Policy specifies mechanisms for the protection of information sent or retrieved through email. In addition, the policy guides representatives of Crediton Town Council in the acceptable use of email. For this policy, email is described as any computer-based messaging including notes, memos, letters and data files that may be sent as attachments.

Applicability

The Email Security Policy applies to all Crediton Town Council employees, councillors, contractors, volunteers and any other person using or accessing Crediton Town Council information or information systems. Exceptions to this policy must be approved by the Town Clerk.

Policy

Authorised users are required to adhere to the following policies. Violators of any policy are subject to disciplinary actions, up to and including termination.

The following items are the council policy statements for Access Controls:

- All email on the Crediton Town Council information systems, including personal email, is the property of Crediton Town Council. As such, all email can and will be periodically monitored for compliance with this policy.

- Email is provided to the users of Crediton Town Council primarily to enhance their ability to conduct business.
- E-mail security is provided by Fusemail email security, spam and virus filtering, email archiving and hosted Exchange.
- Terminated employees will have all email access immediately blocked.
- Users who leave the Council will have all new emails automatically forwarded to the Town Clerk for 30 days.
- The Town Clerk is responsible for disseminating stored emails to the appropriate party. Thirty days after the date of termination, the former employee's mailbox will be permanently removed from the system.

The following items are the council policy statements for Content:

- Use of profane, inappropriate, pornographic, slanderous or misleading content in email is prohibited.
- Use of email to spam (ie, global send) is prohibited. This includes the forwarding of chain letters.
- Use of email to communicate sexual or other harassment is prohibited. Users may not include any words or phrases that may be construed as derogatory based on race, colour, sex, age, disability, national origin or any other category.
- Use of email to send unprofessional or derogatory messages is prohibited.
- Forging of email content (ie, identification, addresses) is prohibited.
- All outgoing email will automatically include the following statement: 'This email and any files transmitted with it are intended solely for the person to whom it is addressed. It may be confidential and also legally privileged. If you are not the intended recipient, please notify the sender and delete the message from your system immediately. Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any E-mail sent to or from this address may be accessed by someone other than the recipient for system management and security purposes. Senders and recipients should be aware that emails and their contents may have to be disclosed in response to a request made under UK Data Protection and Freedom of Information legislation. This email message has been scanned for the presence of computer viruses. However, Crediton Town Council does not accept any liability in respect of damage caused by any virus that is not detected.'

The following items are the council policy statements for Usage:

- Any email activity that is in violation of policy statements or that constitutes suspicious or threatening internal or external activity will be reported.
- When sending email, users should verify all recipients to whom they are sending the message(s).
- Be aware that deleting an email message does not necessarily mean it has been deleted from the system.

PERSONAL EQUIPMENT POLICY

This policy provides guidelines for using corporate IT support resources for personally owned equipment and related software including, but not limited to: notebook computers, desktop computers, personal digital assistants (PDAs), smartphones and mobile phones.

Applicability

The Personal Equipment Policy applies to all Crediton Town Council employees, contractors, vendors and any other person using or accessing Crediton Town Council information or information systems. Exceptions to this policy must be approved by the Town Clerk.

General Policy

Crediton Town Council recognises that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of corporate resources, human or otherwise, for personal gain must be monitored closely.

As a general rule, employees of Crediton Town Council will not use or request corporate IT resources in the use, network connectivity or installation of their personally owned equipment or software.

Personally owned notebooks and desktop computers will not be granted direct physical access to the network. Employees that wish to access the Crediton Town Council network from a remote location using their personally owned computer may do so using only authorised software and only with the approval of the Town Clerk.

PDAs and smart phones, which include devices using BlackBerry®, iPhone®, Windows Mobile®, Android®, Linux® and Palm® technologies, will be supported according the following rules:

- Employees are responsible for learning, administering, installing and setting up their own PDAs or smartphones.
- Corporate IT resources should not be used for assistance in the basic operation of these devices.

VIRUS, HOSTILE AND MALICIOUS CODE SECURITY POLICY

The intent of this policy is to better protect Crediton Town Council assets against attack from destructive or malicious programmes.

- Any public domain, freeware or shareware software will be evaluated by the Town Clerk prior to installation on any company resource.
- No unauthorised software will be downloaded and installed on end user machines without express approval from the Town Clerk.
- System users will not execute programmes of unknown origin, as they may contain malicious logic.
- Only licensed and approved software will be used on any Council computing resource.
- All licensed software will be write-protected and stored by the Town Clerk.
- Crediton Town Council users will scan all files introduced into its environment for virus, hostile and malicious code before use.
- All website forms are sanitised at browser and server.
- Website statistics are checked on a monthly basis to help identify cyber-crime.
- The Cosmic IT team will ensure that Crediton Town Council obtains and deploys the latest in virus protection and detection tools. Current software installed: Webroot Antivirus protection.
- All information systems media, including disks, CDs and Universal Serial Bus (USB) drives, introduced to the Crediton Town Council environment will be scanned for virus, hostile and malicious code.
- All emails will be scanned for virus, hostile and malicious code.

- All internet file transfers will be scanned for virus, hostile and malicious code.
- The unauthorised development, transfer or execution for virus, hostile and malicious code is strictly prohibited.
- All users will report any suspicious occurrences to the Town Clerk immediately.
- All council systems will be protected by a standard virus protection system.
- Virus engines and data files will be updated on at least a monthly basis.
- Viruses that are detected on a user's workstation will be reported to the Town Clerk immediately for action and resolution.
- Anomalous behaviours of any software programme will be reported to the Town Clerk and/or the Cosmic IT team immediately.

APPENDIX ONE

Cyber Security Breaches
What to do!

Crediton Town Council has used the advice provided on the South West Cyber Security Cluster site and adapted this to suit the needs of the Council

Website Hack

First steps – immediate action

1. Contact Pure Systems straight away on 01363 777014 or support@puresystems.co.uk and ask them to switch site to maintenance mode, or remove access.

Who to contact

1. Report to Town Clerk and contact Pure Systems as soon as you can on 01363 777014 or support@puresystems.co.uk.
2. Contact your host if they are different business/organisation.

Generally, they will review the incident immediately and are likely to roll back the server, then review the code and or database to resolve the issue.

Follow up action

1. Understand if it's the website or database that has been compromised.
2. Speak with Pure Systems, find out how it happened and understand how they resolved the issue.
3. Check your website software is kept up to date.
4. Change any admin passwords for the site, and for FTP access.
5. Run a security checking program on the site – e.g. Security Review or Hacked module for Drupal, Sucuri for WordPress.

Next steps

1. Has any sensitive data been taken? If so, you need to inform the ICO and every individual.
2. Has other valuable, or useful information been stolen, like passwords to your site? Users tend to use similar passwords.
3. Expect a second attack and be prepared - Review the changes made, are there any other ways to prevent a further attack? and check your backup copy.
4. Inform Action Fraud.
5. Consider whether you need a third party security audit/review.

Ransomware Attack

What is a Ransomware Attack?

You click on a link or open an attachment which sets off a process resulting in your files being encrypted and you receive a demand for payment to release them.

First Steps:

1. Unplug from network - pull out network cable to stop ransomware encrypting more files.
2. Disconnect from Wi-Fi network: Turn Wi-Fi Off.
3. Turn off machine as soon as possible.
4. Do not pay any money.

Who to Contact

1. Report to Action Fraud on 0300 123 204 or actionfraud.police.uk.
2. Contact your Project Cosmic IT Team.

Recover from a ransomware attack

1. Take Machine to Project Cosmic IT Team for them to rebuild.
2. Restore files from a back-up that was not connected to the machine at the time of the attack.
3. You could try and find the key to decrypt the files. Nomoreransom.org (a project being run between Law enforcement agencies and IT security companies to help victims recover their data without having to pay the criminals. There is approximately 30% chance of finding the right key).

Follow up action - Next Steps

1. Regularly check the external USB back-ups to ensure they have been successful and rotate two of the three back-ups weekly. Connect the third external USB back-up once every quarter.
2. Be cautious of links in emails and attachments.
3. Only download software, particularly free software from sites, you know and can trust. When possible, verify the integrity of the software through a digital signature prior to execution. Ensure that you regularly update patches for operating system, software, firmware, Adobe Flash, web browsers etc.
4. Regularly update Webroot Antivirus and anti-malware protection and carry out regular scans.
5. Disable macro scripts for email files. Office viewer software for opening Microsoft Office files might also be a consideration.
6. Ensure that you remove admin rights from users, and restrict the use of this.
7. Prevent or restrict the execution of programs in locations such as temporary folders used for internet, or Zip files (compression/decompression programs) including those located in the AppData/LocalAppData folder.

Next steps

Ensure Council Staff are trained in understanding the threats from ransomware, links in emails and attachments that might infect machines.

Phishing Attack

What is it?

A Phishing email is one designed to make you click on a malicious link. This could encourage you to:

- divulge personal information such as passwords or bank information.
- download malicious software such as spyware on to your device.
- install ransomware which locks your files and will only release them when you pay money.
- May encourage you to make a payment to a criminal believing it is a real invoice or email request.

It could be sent by an automated system or it could be more targeted attack. A more targeted attack will identify you and aim to encourage you to click on a link that is particularly interesting or relevant to you.

First steps

1. If you have clicked on a link and divulged your personal bank information, contact your bank immediately, the emergency details will be on your card and change your password for a strong password.
2. If you have downloaded malicious software follow the advice on page 9 (Fake Microsoft Calls).
3. If you have ransomware on your machine follow advice on the previous page.
4. If you have made a payment then contact your bank or credit card company immediately.

Who to contact

1. Contact your bank if you have a made a payment.
2. Contact Action fraud.

Next steps

- This is an attack which relies on people's natural curiosity to tempt them to follow a link. The best guard against this is education.
- Regularly check the external USB back-ups to ensure they have been successful and rotate two of the three back-ups weekly. Connect the third external USB back-up once every quarter. Be cautious of links in emails and attachments.
- Ensure that you regularly update patches for operating system, software, firmware, Adobe Flash, web browsers etc.
- Regularly update Webroot Antivirus and anti-malware protection and carry out regular scans.
- Disable macro scripts for email files, Office viewer software for opening Microsoft Office files might also be a consideration.
- Ensure that you remove admin rights from users, and restrict the use of this.
- Prevent or restrict the execution of programs in locations such as temporary folders used for internet, or Zip files (compression/decompression programs) including those located in the AppData/LocalAppData folder.

DDoS Attack

What is it?

Distributed Denial of Service attack – A large amount of data sent via the internet to either your website, or internet facing company perimeter, with the sole purpose of causing your systems to shut down, due to not being able to handle such large numbers of requests simultaneously.

A DDOS attack is often conducted by hundreds or thousands of compromised machines, typically sending data to your website, or network perimeter. These attacks often come from already compromised machines, and run automatically.

A DDOS attack is quite often the mask or smoke to cover a separate attack on your systems, while you are concentrating your efforts to the DDOS attack.

Look out for

1. Website down.
2. No access to website management.
3. Slow response, or loss of internet access.

First Steps

1. Contact Pure Systems straight away on 01363 777014 or support@puresystems.co.uk and ask them to switch site to maintenance mode, or remove access.
2. Call your internet service provider (ISP) and tell them that you are under attack.
3. Call any other 3rd party's that may be responsible for service delivery, or perimeter security management, and let them know that you are under attack.
4. Capture as much information as possible:
    a) Time of event.
    b) Traffic statistics, if possible, to show traffic throughput.
    c) Server logs.

d) Event characteristics, is it late at night, early morning, all day, all night, etc.

5. Monitor all other systems, and be vigilant to any changes that might take place or are put on your systems, during or soon after the DDOS event.

Who to Contact

1. Report to action fraud 0300 123 2040 as soon as possible.
2. Contact ISP, Web hosting company.
3. Contact any customers/clients if you have experienced a data loss.
4. Inform ICO as necessary.

Follow up action

1. Check all other critical systems and backend databases, taking note of any system changes or modifications.
2. Look to mitigate the issue by having in place a temporary site that you can switch to if you find yourself under attack in the future.

Next steps

1. Engage expert advice to help mitigate the issues, and implement a resilient solution that will limit any DDOS reoccurrence:
    a) Cloudflare
    b) Akami
    c) DOS Arrest
    d) Incapsula
2. Maintain a risk register and update any disaster recovery plan to include a DDOS survival plan.

Further steps

Get Safe Online top tips for protecting your business from a DDoS:

- Consider the likelihood and risks to your organisation of a DDoS attack, and put appropriate threat reduction/ mitigation measures in place.
- If you consider that protection is necessary, speak to a DDoS prevention specialist.
- Whether you are at risk of a DDoS attack or not, you should have the hosting facilities in place to handle large, unexpected volumes of website hits.

Continually train Council staff to help them to be aware of phishing emails. Often these can be very convincing but there may be clues such as spelling mistakes or having an urgency about them to encourage you to click on them.

Before you click on any link hover over it and see where they direct you before you click. If links are to a company's website, visit the company's website yourself rather than click on the link.

Take your time opening emails, always look for any typos, capital letters where there should be lower case, extra spacing and full stops missing. Be aware of fuzzy or unclear logos. Take your time rather than respond to any 'urgent action' type emails.

Social Media Hack

What is it?

When someone takes control of your social media account such as Facebook or Twitter. This could mean there are posts on your social media page that you did not make.

First Steps

1. Try first to change the password if you can get into the account.
2. If this is not possible then contact the provider for help, see who to contact below.
3. If your Google account has been hacked this will be more complicated as it may be linked to several accounts, try to log into your Gmail account change the password, if you are unable to log follow contact details below.

Who to contact

1. Facebook Account recovery
2. Instagram help
3. Gmail account help
4. Linked in
5. Twitter
6. Contact Action fraud

Next steps

1. Once you have taken back control of your social media account set up two factor authentication to make it more difficult for hackers in the future.
2. Use password that is more difficult to hack

Follow up

- Facebook enables you to set up login notifications. Go to settings, select security, then Login Notifications and set up email or text send you an alert when your account is accessed by a computer or mobile that you have not used before.
- You can also set up two factor authentication by selecting settings and then Login Approvals and follow the links.
- Set up two factor authentication on your other social media accounts in a similar way.

PBX Dial Through Fraud

What is it?

Your phone system being compromised and a multitude of premium calls being put through your system. The first time you may know this has happened is from an unusually high phone bill.

First Steps

1. Disconnect phone system immediately.
2. Contact BT to log date and time of suspected attack so they can monitor outbound call destinations.

Who to Contact

1. Action Fraud.
2. Call BT and set up call logging on any system that is suspected to be part of fraud.

Follow up action

1. Restrict calls to destinations that should not normally be called, premium rate calls, overseas or any directory enquiry services.
2. Set voicemail up securely on your system and disable voicemail access from outside lines.
3. Set up secure pins for access to remote voicemail.
4. Put restrictions on any extension that must have access to outside line using voicemail.

Next steps

1. Disallow access to the administration facility of the PBX. Configure any networked telephone exchanges to restrict support companies from calling in from outside the PBX to dial calls as if from one of the extensions.
2. Regularly change to random passwords for the administration interface.
3. Configure administration modem to only answer from a single telephone number.
4. Avoid auto features and ensure interactive voice response and auto attendant options for accessing outside lines are removed.
5. Ask telephone provider to set up monitoring and to cut off services if they exceed pre-agreed thresholds.

For further advice from Get Safe Online

Email Hack

What is it and why is it important?

- Why this is critical: your email is the gateway to many password change mechanisms. If your email is compromised then every website or service you have authenticated access to via your email is vulnerable though 'Forgotten Password' recovery mechanisms, unless you use 2 factor authentication and your mobile is still secure. This is a hacker technique called daisy-chaining; access to your email allows daisy-chained access to any associated account.
- If your email account has been compromised you might be unable to log into your email on your device.
- You are unable to access your web mail with your user name and password.

There are several types of email hack:

1. Spambot – an automated system which takes control and uses your email account to send spam. Whilst annoying, it will not be clever enough to change your account settings so that you are locked out.
2. Phishing – simple way to fool someone to give you log in details.
3. Keystroke capturing – implementing malicious software which will log all key strokes on your keyboard.
4. Password guessing – knowing details around your victim, or forcing passwords that are easy to guess and allowing the attacker to gain access to your online accounts.

First Steps

1. Change your password on your email account if a spambot has taken control and is sending spam from your account.
2. If you are unable to do this, there is chance that a real person has taken control of your account, they may have changed your password, you can reset this by going to your sites log-in area and the "forgot your password link" and can have the new password sent to a different email account if you have set one up previously.
3. It is possible that the hacker has changed your security questions and recovery email and can get back in whenever they want to. You will need to log an incident with your account provider.

Who to Contact

1. Action Fraud.
2. Outlook account service provider – technical support team

Follow up action

1. If you have responded to a suspicious email then log into your legitimate account and change the password.
2. Delete suspicious emails that might encourage you to respond to password reset information.
3. Use a separate email account and warn some of your key contacts to be wary of any suspicious emails.

Fake Microsoft Support Call

What is it?

You receive a call from someone from Microsoft Helpdesk telling you that they have discovered a problem with your PC. They ask you if you are near your machine, ask you to log in. They use a 'let me in' type link which allows them to take control of your machine.

They can then either put some malicious software on your machine which could provide them with information about bank passwords etc. Alternatively, they tell you that you have a major problem, and will fix it for you, often by selling you some form of 'anti-virus' software, usually at an extortionate price. Or worse a combination of both.

First Steps

How to respond: Hang up…it's a scam!

If you have already allowed access or responded you may have already downloaded malicious software onto your system or allowed access to your computer.

1. Change your computer's password.
2. Change the password on your main email account.
3. Change the password for any financial accounts, especially your bank and credit card.
4. Use Webroot Antivirus scanner to find out if you have malware installed on your computer.

Advice from Microsoft

"If you are using an old version of Windows (Windows 7, Vista or XP), Install Microsoft Security Essentials. (Microsoft Security Essentials is a free program. If someone calls you to install this product and then charge you for it, this is also a scam.)

Note: In Windows 8, Windows Defender replaces Microsoft Security Essentials. Windows Defender runs in the background and notifies you when you need to take specific action. However, you can use it anytime to scan for malware if your computer isn't working properly or you clicked a suspicious link online or in an email message."

Who to Contact

Report to Action Fraud

Follow up action

Make sure you make anyone you know who may be susceptible to this aware of this scam and train your staff not to respond.