Summer Valley PCs

What to Do After a Scam Call

Have you received a suspicious phone call from someone claiming to represent your bank, Amazon, Microsoft, your internet provider or another trusted organisation?

Scammers often impersonate well-known companies to trick people into sharing personal information, making payments or allowing remote access to their computers.

If you think you've been targeted by a scam, don't panic.

There are steps you can take to protect your money, personal information and computer. This free guide from Summer Valley PCs explains what to do next.

1. Disconnect from the internet

If you've allowed a scammer to access your computer remotely, disconnect it from the internet immediately. Turn off Wi-Fi or unplug the Ethernet cable connecting your computer to your router. This can help prevent the scammer from continuing to access your computer. If you cannot shut down your computer normally, press and hold the power button for approximately 10 seconds until the computer switches off. Important: You don't need to disconnect your computer if you've only received a suspicious phone call and haven't allowed anyone remote access.

2. Contact your bank immediately

If you've given the scammer your bank details, card information, passwords or access to your online banking, contact your bank immediately. Explain what happened and ask them to check your accounts for suspicious activity. Your bank may need to block your card, secure your account or stop any unauthorised payments. Important: Contact your bank using the number on the back of your bank card or its official website, never a number provided by the scammer.

3. Avoid using the affected computer for banking or changing passwords

If a scammer has accessed your computer remotely, don't use it for online banking, shopping or entering passwords until it has been checked. The scammer may have installed software that allows them to monitor your activities or access your personal information. Important: Use a different, trusted device, such as your mobile phone or another computer, for important services.

4. Change your important passwords

If you've shared passwords with a scammer or allowed them access to your computer, change your important passwords as soon as possible. Always use a different, trusted device. Start with your email account, followed by online banking, shopping accounts and other important services. Use a different, strong password for each account. Where available, enable two-factor authentication (2FA) for extra security. Important: Never change passwords on a computer that may still be compromised.

5. Have your computer checked

If you've allowed a scammer to access your computer remotely, it's important to have it professionally checked before using it again. Summer Valley PCs can check your computer for remote access programs, unwanted software and any changes a scammer may have made. Even if you've removed the remote access program yourself, this doesn't necessarily mean your computer is safe. A thorough security check can help identify potential threats and reduce the risk of further problems.

6. Report the scam

If you've been targeted by a scam, it's important to report it, even if you haven't lost any money, as reporting helps the authorities investigate fraud and protect others; in England and Wales you can report it to Report Fraud online at www.reportfraud.police.uk or by calling 0300 123 2040.

Need help after a scam call?

If you're worried that someone may have accessed your computer, Summer Valley PCs can help identify suspicious software, check for security problems and advise you on the next steps. **Call us on 01792 538 168 or 07989 641 993.**