Computer Technical Support Scams

Background

Fraudsters often use the names of well-known companies to commit their crime, as it makes their communication with you seem more legitimate. Common scams that use brand names include:

- receiving a phone call from 'Microsoft Tech Support' to fix your computer.
- receiving unsolicited emails from software providers regarding security updates.
- being asked for your credit card information to 'validate your copy of Windows'.
- being told you have won the 'Microsoft Lottery'.

What actually happens?

Fraudsters cold-call victims pretending to be from well-known broadband providers (or other well-known firms such as BT or Apple), claiming that the victim has a problem with their computer, broadband router or internet. The fraudster directs the victim to a website to download a tool that allows the caller remote access to the victim's computer.

The fraudster then appears to make a number of 'fixes' to the victim's computer when in fact, they are accessing the victim's personal information, often by installing malware or a virus on the computer. Alternatively, victims are persuaded to log into their online banking to receive a refund from the broadband provider or firm as a form of compensation. This allows the fraudster access to the victim's bank account, and the ability to move funds out of the victims account into the fraudsters account.

Recent reports also advise that fraudsters have been using emails or internet browser pop-up windows to initiate contact with victims.

Advice to avoid Computer Technical Support Scams

Firms that are being impersonated warn that they do not send unsolicited emails or make unsolicited phone calls to request personal or financial information, to validate software, to send security updates or to fix your computer. Fraudsters make these calls to try to steal from you and damage your computer with malware or viruses.

- If you receive such communication, delete the email, close down any pop-ups or hang up the phone.
- Never install any software, or grant remote access to your computer, as a result of a cold call.
- If you have granted remote access to your computer, seek professional technical support to remove any unwanted software or malware/viruses.
- Treat all unsolicited phone calls with suspicion and don't give out any personal or financial information.
- Hang up on any callers that claim they can get your money back for you.
- If in doubt about a request for information or a request to click links in an unsolicited email, don't open the email, just delete it.
- If you think the contact could actually be from the firm, contact them directly using the phone numbers obtained from their contract, their website or other trusted sources.
- If you have made a payment, contact your bank immediately to prevent any further losses.

If you think you've been a victim of fraud, report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.

Prepared by:- Gillian Baker, Financial Risk Management Lead

For and on behalf of Hymans Robertson LLP