Weekly Fraud update from West Mercia Police - Economic Crime Unit - 14/03/2023

ANYDESK SCAM

We highlighted this Scam early last year but there have been some recent reports in our area of residents falling victim to this Scam once again.

In one case a text was received claiming to be from telephone number "101" with crime numbers and advising that there had been criminal activity on a bank account. They were then persuaded to download the AnyDesk App which then gave the fraudster access to their bank accounts.

In a second case, the call allegedly came from the victim's bank itself who convinced them to download the AnyDesk app as there had been unusual activity on the bank account. Funds were then removed via the App.

AnyDesk in itself is secure, trusted and used by many people without problem. When installed correctly, It is completely secure and a tool for when IT experts want to work on remote devices without being on-site.

However there have been reports of members of the public receiving phone calls from Scammers asking them to download AnyDesk and then accessing that computer or mobile phone to glean personal details, bank details etc.

If anyone cold calls you and asks you to download AnyDesk you are advised not to respond and hang up on the caller. They could use this software to steal your money.

What to do if you've given a scammer remote access to your device

· First and foremost, take back control of your device – if you can still see your screen, there should be a disconnect button enabling you to end the session but as a precaution, turn off Wi-Fi at the router or unplug the network cable to fully disconnect from any external connection.

· Tell your banks immediately if there is a chance they have been compromised and report the crime to Action Fraud.

· Once your device has been switched back on, you can remove the software (check for recently installed programs/downloads) and any other apps that may have been installed by the scammer while they had remote access.

· You should reset all passwords for online accounts (current accounts, savings, email etc.) and enable two-factor authentication where possible.

· If you have security software, ensure it has all new and recent updates – then run a full security scan.

See also: https://anydesk.com/uk/abuse-prevention

BEWARE SCAM EMAILS WITH ATTACHMENTS

Please be also aware of scammers using “OneNote" attachments on fake emails. Whilst in the past they have tended to use Excel and Word documents as attachments to infect computers with Malware, since this was now less effective they are now resorting to OneNote.

The scam OneNote attachments are easily recognised as they use an out of date fake logo for One Note, the genuine logo should be coloured purple in all areas, and not just on the “N” motif.

Take Five To Stop Fraud

- **Stop:** Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge:** Could it be fake? It’s okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect:** If you think you’ve been a victim of fraud, contact your bank immediately and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.

For further information visit:

https://www.actionfraud.police.uk/

https://takefive-stopfraud.org.uk/