Subject: Over 22,000 email and social media account hacked [#233424545]
Date: Monday, 18 March 2024 at 17:46:39 Greenwich Mean Time
From: Wiltshire and Swindon Community Messaging <alert@neighbourhoodalert.co.uk>
To: Elizabeth Martin <Parish.Clerk@lynehamandbradenstoke-pc.gov.uk>

COMMUNITY MESSAGING

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Urgency: 3 2 1

CRIME PREVENTION

Over 22,000 email and social media account hacked

Dear Subscriber,

Data from Action Fraud, the national fraud and cybercrime reporting service, shows that **22,530 people** reported that their online accounts had been hacked in 2023, with victims losing a total of £1.3 million.

How are accounts hacked?

On-platform chain hacking

This is when a fraudster gains control of an account and begins to impersonate the legitimate owner. The goal is to convince people to reveal authentication codes that are sent to them via text. Many victims of this type of hacking believe it's a friend messaging them, however the shared code was associated with their own account and the impersonator can now use it to access their account. Usually when an account is taken over, fraudsters monetise control of the account via the promotion of various fraudulent schemes, while impersonating the original account owner.

Leaked passwords and phishing

The other predominant method of hacking reported is leaked information used from data breaches, such as leaked passwords, or account details gained via phishing scams. This becomes prevalent as people often use the same password for multiple accounts, so a leaked password from one website can leave many of their online accounts vulnerable to hacking.

How to secure your accounts

- **Use a strong and different password** for your email and social media accounts. Your email and social media passwords should be strong and different from all your other passwords. Combining three random words that each mean something to you is a great way to create a password that is easy to remember but hard to crack.
- **Turn on 2-Step Verification (2SV)** for your email and social media accounts. 2-Step Verification (2SV) gives you twice the protection so even if cyber criminals have your password, they can't access your email or social media account. 2SV works by asking for more information to prove your identity. For example, getting a code sent to your phone when you sign in using a new device or change settings such as your password. You won't be asked for this every time you check your email or social media.

If you live in England, Wales and Northern Ireland and have been a victim of fraud or cybercrime, report it at www.actionfraud.police.uk or by calling 0300 123 2040. In Scotland, victims of fraud and cybercrime should report to Police Scotland on 101.

If you receive a suspicious email, you can report it by forwarding the email to: **report@phishing.gov.uk**.

Find out how to protect yourself from fraud: Gov.uk/stopthinkfraud

(If you found the information in this email useful, please forward it to your friends, family and colleagues)

Message Sent By
Action Fraud
(Action Fraud, Administrator, National)

To reply or forward please use the below or these links: Reply, Rate, Forward / Share.

Reply Useful or not? Share Settings

To login to your account click here, to report a fault click here, or unsubscribe

neighbourhood ALERT ©

CYBER ESSENTIALS CERTIFIED PLUS

You are receiving this message because you are registered on Wiltshire and Swindon Community Messaging. Various organisations are licensed to send messages via this system, we call these organisations "Information Providers". Please note that this message was sent by Action Fraud (NFIB) and that Action Fraud (NFIB) does not necessarily represent the views of Wiltshire and Swindon Community Messaging or other Information Providers who may send you messages via this system.

You can instantly review the messages you receive and configure which Information Providers can see your information by clicking here, or you can unsubscribe completely, (you can also review our terms and conditions and Privacy Policy from these links).

This email communication makes use of a "Clear Image"(gif) to track results of the email campaign. If you wish to turn off this tracking for future emails, you can do so by not downloading the images in the e-mail itself. All links in the body of this email are shortened to allow click through monitoring.

VISAV Limited is the company which built and owns the Neighbourhood Alert platform that powers this system. VISAV's authorised staff can see your data and is registered with the Information Commissioner's Office as the national Data Controller for the entire database. VISAV needs to see your data in order to be able to manage the system and provide support; it cannot use it for commercial or promotional purposes unless you specifically opt-in to Membership benefits. Review the website terms.