Jeremy Collins

From: alert@neighbourhoodalert.co.uk
Sent: 04 June 2019 15:23
To: bucklandnewtonwebmaster@gmail.com
Subject: Staying Safe Online - New Web Address For More Info 04/06/2019 15:23:29 [272625]

Priority: 5 4 3 2 1

LOCAL NEWS

Staying Safe Online - New Web Address For More Info

Hello

We had a fantastic response to our recent message, in which Dorset Police Cyber Protect Officer Chris Conroy gave advice about how to avoid falling prey to online fraudsters.

Unfortunately, many people weren't able to access the web link contained within the article. If anyone now wants to find more information about staying safe online, please try visiting this page:

https://www.dorset.police.uk/help-advice-crime-prevention/scams-fraud-cyber-crime/cyber-crime/

Or you can get in touch with Chris and his team directly by e-mailing cybercrimeprevention@dorset.pnn.police.uk.

If anyone didn't get a chance to read the original article, it's included below:

My name is Chris Conroy, and I am the Cyber Protect Officer for Dorset Police.

It's my job to make sure the people of Dorset are best placed to defend themselves against cyber crime. You'll usually find me out and about delivering presentations to community groups and businesses around the county, or over on our social media pages, giving useful tips on how to stay safe online.

However, today you find me here, writing my first guest blog for the Police and Crime Commissioner. And what better way to start it than by bringing you some good news?

Last year, a whopping £354 million was lost to what's known as "authorised push payment fraud". This isn't the good news, obviously… that's coming shortly.

These are scams in which customers are tricked into actually making a payment, rather than the money simply being stolen. Historically, banks would only pay out if they were clearly at fault. As such, only £83 million was recovered, meaning the UK public lost £251 million.

This week, however, marks a turning point for victims of fraud, as a new voluntary code takes effect. From now, payment providers who are signed up to the voluntary code will judge each case against a set of criteria to determine whether a customer should be reimbursed after falling for a scam, and anyone who has taken reasonable care, or has any element of vulnerability, is much more likely to receive a refund of the lost money.

Eight major banks, covering 17 brands, have committed to implementing the code with immediate effect. They are:
• Barclays
• HSBC (including First Direct and M&S Bank)
• Lloyds (including Halifax, Bank of Scotland and Intelligent Finance)
• Metro Bank
• Nationwide
• RBS (including NatWest and Ulster Bank)
• Santander (including Cahoot and Carter Allen)
• Starling Bank

TSB have taken this one step further, and state that they guarantee a refund for anyone who is an innocent victim of fraud. Pretty good, right?

It's really encouraging to see banks stepping up and helping victims of fraud, but it is worth pointing out that the code does not apply in cases where victims have been "grossly negligent". At this time, it's not entirely clear what constitutes gross negligence, so it seems as good a time as any to remind people how to avoid falling victim in the first place.

First and foremost, stop and think. A common tactic used by fraudsters is to use social engineering techniques to get you to act against your better judgement. A bank won't pressure you to act fast, or apply time limits to anything. If you feel you are being rushed to hand over information, stop. Do not let anybody make you do something you don't entirely understand, or aren't comfortable doing.

It's worth remembering that your bank will not contact you out of the blue to ask for sensitive information like your PIN or password. Nor will they ask you to move money into a new account.

Take care with emails. If you receive an unsolicited email, be wary of clicking any links or attachments. "Phishing" emails are a common tactic used to gather sensitive information from victims. Always question uninvited approaches asking for personal details, in case it's a scam.

If you receive an unexpected message from your bank, or a company, consider calling them directly using a telephone number you know and trust, rather than by calling a number in an email or text message.

For further advice about all things cyber crime, get in touch. And if you are part of a community group, or a local business, feel free to get in touch to arrange a cyber crime prevention talk! I'm available daytime, evenings and weekends, and it's

completely free of charge.

I hope to hear from you soon! Until next time, thanks for reading.

Chris

Message Sent By
PCC Communications (Dorset Police and Crime Commissioner, Communications and Engagement, Dorset)

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

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