Jeremy Collins

From:	alert@neighbourhoodalert.co.uk
Sent:	11 June 2019 16:30
To:	bucklandnewtonwebmaster@gmail.com
Subject:	How To Stay Safe On Social Media - Part One 11/06/2019 16:30:24 [273615]

Dorset ALERT

Dorset Police

Priority: 5 4 3 2 1

LOCAL NEWS

How To Stay Safe On Social Media - Part One

This month, Dorset Police Cyber Protect Officer Chris Conroy looks into how social media can be used against us – and what we can do to protect ourselves.

It was my birthday a few days ago. 32. Not a big birthday, admittedly, but that didn't stop the stream of notifications from my friends and family. I got some really lovely messages on my Facebook, some mildly offensive ones, and a whole load of two word "happy birthday" posts. Among all the noise, however, one message stood out.

It was a simple "Hello. How are you doing today?" and it came from a family member. That in itself, of course, isn't that strange. Sure, it's not a conventional "happy birthday", but we'll let that slide.

It was what came next that threw me.

"I'm just wondering if you heard about the good news going on. It's all about the PCH program."

It goes on… Apparently, the PCH program have randomly selected me, as well as my family member, and I am in line to receive $90,000! Well, happy birthday to me!

But, of course, something isn't quite right. The language he's using. The prize being in dollars. The fact there are now two accounts in his name in my messages… It becomes pretty clear their account has been cloned. Their name, their profile picture, their basic details… everything had been taken in order to set up a fake account.

That account was made for one purpose. To defraud everyone in that family member's list of friends out of their hard earned cash.

Thankfully, your friendly neighbourhood Cyber Protect Officer didn't fall for it. But what if the fraudster had targeted someone else? Someone a little more trusting, or a little less cyber aware?

Cybercriminals can be incredibly convincing, and it’s easy to see how some people fall victim. Especially when the messages appear to be coming from a trusted contact.

So I thought I’d take the time to put together a brief summary of the ways hackers and scammers use our social media profiles against us.

Fear not! It might make for pretty bleak reading, but there are tips along the way to make social media as safe as possible!

Here we go…

1) Harvesting details from our profiles.

Have you ever taken the time to consider what you’re putting on your social media profiles?

Sometimes the hackers don’t have to hack at all. Sometimes we hand our information over on a silver platter.

Some people are surprisingly liberal with what they share on social media, with dates of birth, addresses and phone numbers being quite common. If people share too much data, scammers can piece things together to stand a reasonably good chance of impersonating someone.

Another thing to consider is your password. I’d like to think everyone is using long, strong, complex passwords, but the reality is most are probably still using some combination of a name (a child, pet, or place for example) and the year they were born. Can people figure those details out from your posts? All those puppy pictures and birthday messages could be giving away more than you thought.

Solution:

Think about what you’re sharing. If you wouldn’t share it with a stranger, don’t share it on social media. Take the time to check your privacy settings. Setting your account to private means only approved contacts or friends can see what you post, meaning you’re safe from prying eyes.

2) Fake friends:

You’ve got your profile set to private, and no one but trusted friends and family can see what you’re posting. Excellent!

This, however, is a relatively small barrier for a scammer to overcome if you don’t pay attention to your friend requests.

I’ve lost count of the times I’ve received friend requests from people around the world. Maybe I’ve prematurely shut the door on some wonderful friendships. More likely though, I’ve just avoided the start of a sextortion scam, or blocked someone from snooping on my profile.

Sextortion - for those who aren’t aware - is a particularly nasty scam that can have devastating consequences. It relies on a victim accepting a friend request and getting into conversation with their attacker. The attacker pretends to be an attractive young male or female, and builds up a rapport with their victim.

As the trust builds, the scammer tries to convince the victim to remove their clothes in front of their webcam, or more. Then the scammer strikes. They tell their victim they've recorded everything, and a demand is made for a sum of money, with the threat of posting the video online if they don't pay.

The ramifications can be huge, with responses ranging from mild embarrassment and financial loss to suicide.

Solution:

Do not accept friend requests from people you don't know and trust, and be guarded with what information you share with strangers.

Do not allow anyone to pressure you into doing something you're not comfortable with. If you are unfortunate enough to fall victim to a sextortion scam, we do not recommend paying. There is no guarantee the scammer won't come back and demand more money. Call the police in confidence on 101, and we can help.

3) Phising and Malware:

Phishing is something we more commonly associate with emails. Badly worded messages promising payouts from a Nigerian General, refunds due from HMRC, or mysterious purchases made on our Amazon accounts, for instance.

However, cybercriminals have cottoned on to the fact that social media is a veritable goldmine of potential victims. All a phishing attack needs to guarantee success is enough victims to target. Eventually, they'll find someone who will fall for their scam.

There are many ways a phishing link can be delivered. On a Facebook newsfeed, a direct message, a post on your wall… the possibilities are endless.

One particular example that sticks in our minds was delivered through a Facebook competition in which users were encouraged to like and share a post for their chance to win an £85 gift voucher for a major supermarket chain.

On doing this, the users were sent a message containing a link supposedly taking them to a site from which they could download their gift voucher. But clicking this link actually took them to a website that tried to install malicious software on their computer.

Solution:

Be careful where you click. Take the time to check the source of any link you stumble upon, particularly if it's offering something that seems too good to be true.

A quick pro tip - if you hover your mouse over any link or button in an email or website, the true address should be displayed in the bottom corner of your screen. If the link claims to be from a reputable company, but the true address looks wildly different, it's probably a scam.

A quick point about the "like and share" competitions on Facebook – genuine companies often use these to grow their online presence. Don't assume they are all fake. However, at the same time, don't assume they're all real!

Before you like and share, click into the page. Have a look around and see if it looks genuine. The “About” section of any Facebook page will tell you how old the page is, and whether it has been called something different in the past. We’ve seen scam pages change their name from that of a reputable jewelry store to that of a reputable pizza company, which should be a big red flag.

Also, think about how plausible the prize is. Why would a supermarket just give away gift vouchers? Add up all the likes, shares, and potential winners, and they’d be out of pocket by millions!

There you have it. Part one of the six ways social media can be used against us. If you found it interesting, come back next month to find out how criminals take control of our friend’s accounts, how apps can syphon off your data, and how things live on in cyber space, even after being deleted.

In the meantime, if you want to ensure you’re as safe as possible, make sure you use long, strong, secure and unique passwords for your social media accounts. This will help prevent someone guessing their way into your account.

Once your passwords are in order, make sure you turn on Two Factor Authentication. This acts as a safety net. Even if someone gets your password, they can’t get in to your account.

Don’t forget, if you represent a business or community group, you can get in touch to arrange a free, impartial cyber security presentation. Email us at cybercrimeprevention@dorset.pnn.police.uk

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.

Reply Rate Share Print Settings

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

neighbourhood ALERT
Informing & Listening to Communities

CYBER ESSENTIALS PLUS

messages via this system, we call these organisations "Information Providers".

Please note that this message was sent by Dorset Alert .

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 e-mail communication makes use of a "Clear Image" (gif) to track results of the e-mail campaign. If you wish to turn off this tracking for future e-mails, you can do so by not downloading the images in the e-mail itself.