PARKSIDE COMPUTERS

Avoiding Fraud
January 2018

Hello all,

This is the second edition of the monthly newsletter from Parkside Computers. Last month, the article was focused on staying safe online, but do you know about the numerous other threats that can happen (at least, in part), away from your computers and devices, which can still leave you with problems such as loss of data, identity theft, and loss of funds.

At the moment, it seems like people within our area that are being targeted, with local business owners losing tens of thousands of pounds, and even regular people being conned out of thousands. As time progresses, the law is clamping down on these scams, but sadly, they get more and more advanced all the time.

Luckily, there are ways to spot these fraudsters, and with the right knowledge, you can avoid becoming another scam statistic. The way most of these scams are happening at the moment is through a simple phone call, with the caller pretending to be from a reputable organisation, such as your bank, or BT.

The majority of these will have you answer the phone, and trick you into thinking they are who they say you are, using a few simple tricks. If someone says they're from BT, your Internet Service Provider, you may have no reason to believe otherwise, so they'll talk you through what they want you to do.

Most recently, we've had a few reports of callers saying they're from BT, and then they go down one of a few different routes:

1) BT – Your connection is a bit slow and we want to refund you some money for this issue
2) BT – It seems like your computer is infected, allow us to sort the issue
3) BT – It looks like you're not quite connected properly, we'll help get you back online

There are many variations to this, with callers claiming to be from any number of large businesses. Staying vigilant, and knowing what to look out for, could save you from being victimised.

The first thing to know is that if your instinct tells you this isn't quite right, chances are, you're right.

Secondly, and this is a big one (for the BT scams). If they claim they're from "BT Openreach, your internet service provider", you can be sure it's a lie. Openreach are not an internet service provider, they just look after the infrastructure. If a call starts like this, it's not right.

Thirdly, if the call originates from a non-UK number. Now, we all know big companies have call centres overseas, but generally, any call from them will be routed via a UK number. If it's not UK (and you're not expecting a call), don't answer it.

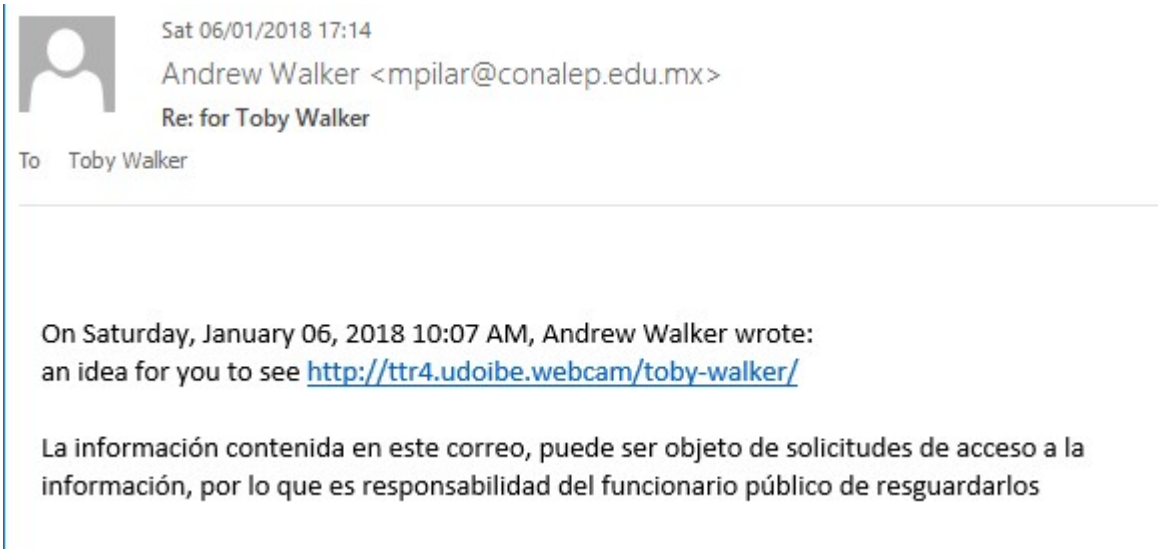
Another thing that should set alarm bells ringing is if the caller wants to take control of your PC. If they ask you to do *anything* on your computer, just ignore them. If you do allow access, my advice would be to take the machine they gained access for a malware removal, and change all your passwords (they may not be compromised, but better safe than sorry). Parkside Computers would be more than happy to assist with this.

The golden rule is to never allow anyone access to your machine unless you know *exactly* who they are. If in doubt, just hang up, and if you'd like to be 100% safe, give one of our friendly team a call.

Unfortunately, it isn't just telephone calls that can catch people out. You may get an email from someone you know with a link to a website. If you're expecting one, chances are, there's no problem. If it seems a bit out of character, it may be worth getting in contact via phone or letter to tell them you have reason to believe their own account has been compromised, and to seek advice and change their passwords.

I, myself, receive emails like this nearly on a bi-weekly basis. At first glance, they look like they have come from a member of my family, made even more possible by the fact we email one another frequently to allow us to keep in contact.

However, a bit of further investigation reveals this is definitely not an email I'm wanting.



Sat 06/01/2018 17:14

Andrew Walker <mpilar@conalep.edu.mx>

Re: for Toby Walker

To Toby Walker

On Saturday, January 06, 2018 10:07 AM, Andrew Walker wrote:
an idea for you to see http://ttr4.udoibe.webcam/toby-walker/

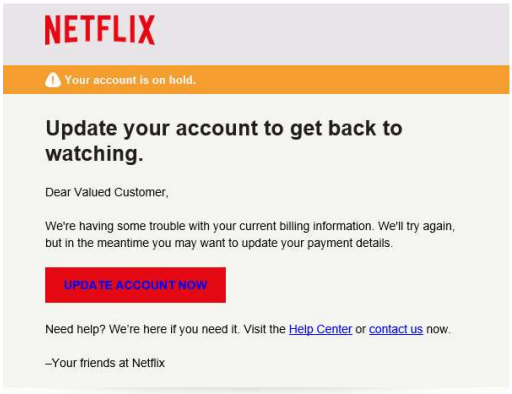
La información contenida en este correo, puede ser objeto de solicitudes de acceso a la información, por lo que es responsabilidad del funcionario público de resguardarlos

Looking at the above email, it appears it has come from Andrew Walker, but if we look at the email address displayed to the right, this is the first sign it's not who it may seem.

Then, the subject line. If it says "RE:", this means it is a reply to an email you have sent. If you haven't sent one, it's likely this is a scam. (Note that occasionally forwarded emails will have RE: in the subject line, so this isn't always definitive.)

The next giveaway is the link. There's definitely something off about it. Probably best not to click it.

These emails can come from large organisations too, such as Netflix. I received this email last year:



NETFLIX

Your account is on hold.

Update your account to get back to watching.

Dear Valued Customer,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

Need help? We're here if you need it. Visit the Help Center or contact us now.

–Your friends at Netflix

There are a few giveaways in this email. The first (which isn't shown in the image), is that it came from a completely wrong email address.

The next is to do with how it is addressed. You would not be contacted by a company that you subscribe to, with the first line being "Dear Valued Customer". It will be addressed to you, by name. If it is addressed to your email address, again, it is a giveaway.

If you're unsure, you can forward them to us to have a look at.

Wishing you all the best for 2018. If in doubt, just don't do it. Contact someone to assist.

Parkside Computers
Arnside
LA5 0HA

01524 761515
info@parksidecomputers.com