Swanley Computers Ltd
40 High Street, Swanley, Kent. BR8 8BQ 01322 284435
www.swanleycomputers.com

How to spot and avoid Computer Scams

This is a short guide, or was but we keep updating it, to help our customers (and anyone else) to spot potential internet threats. It covers the basics of what to look for and how to avoid the more obvious scams that are out there.

There are several Golden Rules to follow and these can be found in the article below.

It's not a definitive guide, nor designed for the more technically minded, but is a useful tool for those who are perhaps not so computer literate, or those who just use their system occasionally. It's also handy for the silver surfers amongst us.

One important piece of advice is to update your Anti-Virus Software (You do have Anti-Virus Software!) daily. This is often done automatically but if you have been away for a few days then make sure you update the software before you check your emails etc. Anti-virus definitions which are out of date will not catch the latest threats. So, it's worth doing and only takes a minute or two.

This document does not include any Internet links to web pages so if you have a copy that does, it's not ours. This guide is updated from time to time. The name of the document incorporates the date so it's easy to tell if its newer than your old one. Also, that way you make sure it's ours and not one hijacked by anyone else ☺

There are 7 common scams that catch people out and these are:

1. Telephone Call Scams
2. Internet Pop Up Scams.
3. Internet Website Scams.
4. Drive By Downloads
5. "How to solve problems sites"
6. Links in emails.
7. Emails with attachments.
8. I have your Password Email (New)

There is a subtle difference between a Virus, Malware and Spyware. It's beyond the scope of this simple leaflet to differentiate between them so for the purposes of this guide we shall regard them as an Internet Threat.

Swanley Computers Ltd
40 High Street, Swanley, Kent. BR8 8BQ 01322 284435
www.swanleycomputers.com

Telephone Call Scams:

The first one is simple easy to deal with and easy to recognise. You get a phone call from a person who states that they are from Microsoft, BT, Talktalk, Virgin, your ISP Provider (the company that provides you with your Internet) or something similar. We have even had reports that they pretend to be from Anti-Virus Companies such as Norton, McAfee, AVG etc. Then they go on to say that your computer is infected, is running slowly or something similar. Helpfully the conmen offer to login to your computer and show you the problem. Having logged in and taken control the fancy looking software reports that you appear to have problems. Most typically they show you the standard Windows Services Screen which shows various services are on and others are off or not running. **This is actually perfectly normal!** They also run software that shows that you badly infected and an impressive looking screen indicates how many infections you have and so on.

The suggestion is made that you pay them to remove it. Some people realise that it's a scam but usually it's too late. The scammers activate a programme which locks you out of your computer and can sometimes make your system unusable.

The best way to avoid this type of scam is to put the phone down or say you don't have a computer, only a tablet. Then **put the phone down**. Job Done. It's really that simple to avoid.

Internet Pop Up Scams

This one is also easy to spot, but also very easy to fall for! There you are surfing the Internet and suddenly a window opens telling you that you are infected. You read the screen and click on the link / help button / more info button / contact us button etc and you are confronted with a screen showing you that your system is awash with infections, Trojans, bad drivers etc and you should call a number for immediate assistance. Or you can download their very handy software to help you remove it, or something similar. Once you do you are infected and it's too late. Your systems slows to a crawl and you are confronted with a multitude of warning messages and pop – up windows.

If you get such a screen – close it. **Don't click on any of its contents**. Simply shut that window down and go to another site.

Internet Web Site Scams

Another easy trap to fall into and can take many forms. Typically, you think you may be infected so you search on the Internet for a solution. For example, you may think you are infected with "Malware" so look it up on the Internet. You locate a site which promises to remove the infections. You download the software and lo and behold a list of nasty infections and spyware and other computer faults gets displayed on your screen**. Lucky you found their site then!** Helpfully it suggests that you purchase this wonderful software and your problems go away. Yes, right. There are a lot of sites out there that are quite frankly fake and software can easily be used to display a whole multitude of problems. Unless you go to the very well known vendors, **steer clear of these ones.**

Drive By Downloads

This is a clever method of infecting your computer, based on the above. Someone sets up a website, which is just a launch pad for infecting your computer. As soon as you visit the page, a programme downloads to your computer and runs. It's that simple. I can give you a personal example. I was looking for a picture of a padlock and used Google to look for images. A suitable image appeared in the list. I clicked on it and a programme tried to download, install and infect my computer. **It really is that easy for you to get infected.** It's important to note that Google are not to blame or responsible for this kind of attack.

Problem Solving Sites

Although there are websites that offer good advice and information (including us!) there are also those sites setup to deceive you. The best policy is not to believe most of what you read on "helpful forums" and seek advice from proper sources. I have seen the most laughable answers to internet infections. Some of it is well intentioned but there is an **awful lot of simply wrong and damaging advice given – most particularly to do with data recovery** – which although off of the subject matter can still be regarded as very damaging to a user needing to get data back, for example.

Links In Emails

A well-publicised problem and it is a bit unusual for people to get caught out. However, it works like this. You get an email from a well-known company or bank. You are informed that there is a problem with your account / it's being upgraded / suspicious activity has been detected or something along those lines. A helpful link has been included for you to visit the company page so that you can login and confirm information. **Ummm, I don't think so!** It would be unlikely that a company would contact you and provide you with a link. If you wanted to check all is well you could login in the usual way by going to the website but ignoring the link in the email. That last bit is most important**. I never click on an email supplied link, ever.**

Emails with attachments.

This is the most damaging threat at the moment and has been in the news as **your computer data becomes encrypted by so called "ransomeware".** Here's how it happens. You open your email programme and see an email from a company saying that they could not deliver a parcel / you have an invoice outstanding, / your refund is attached, / we were sorry to miss you etc. There is also a small file attached often in a "zip" format, and just recently with **.exe or .zop after the file name**. You open the email and within seconds every document, picture, video, music file etc. will be encrypted. You are then confronted with a screen requesting money or your files will remain locked. This is called "ransomware" and although your files can sometimes be retrieved - other times they cannot. **Golden rule is never open an email with an attachment, unless you are expressly expecting it**. My other rule is **never, ever open a zip file**. Files can easily be sent via another medium such as dropbox etc. Much safer, and then you know who it is from.

Swanley Computers Ltd
40 High Street, Swanley, Kent. BR8 8BQ 01322 284435
www.swanleycomputers.com

Fake Update Messages

So, there you are surfing around the Internet and a message comes up telling you that your **Flash Player is out of date**, or similar, and you should **"click here"** to update it. **No, you shouldn't**. If your flash player needs updating, then go to the **Adobe website** and update it from there. Adobe Flash Player (which is used extensively on the Internet) updates usually in the background by itself, so you can ignore the message or visit the site. There are also a lot of other fake message like this.

Another common one is the dreaded **"Your drivers are out of date"** and you should **update them** by going to a useful site…which demands a fee. It is true that drivers are updated from time to time, but generally speaking you don't have to worry. The major components of your computer will often **update themselves via Windows Updates** and driver updates for the other items are hardly crucial and free from manufacturers websites.

Other attempts to get you to click on a link will often involve messages telling you that you need to **backup your data,** (which you should do often), update Internet Explorer, Windows needs updating (automatic for most people) Java is out of date, media player is not loaded, your hard disk is about to break down, and a whole host of others. Ignore the lot of them. If you do need or feel that something needs updating then go directly to the manufacturers website.

I have Your Password Email

Content of email received looks something like this *(in italics)*

You may not know me and you are probably wondering why you are getting this e mail, right? I'm a hacker who cracked your email and devices a few months ago. You have 48 hour in order to make the payment. (I've a unique pixel in this e mail, and at this moment I know that you have read through this email message).To track the reading of a message and the actions in it, I use the facebook pixel. Thanks to them. (Everything that is used for the authorities can help us.) If I do not get the BitCoins, I will certainly send out your video recording to all of your contacts including relatives, coworkers, and so on. Quote ends here:

The email goes on to say that they have recorded me via my webcam etc etc. I don't have one so wrong again!

However, quite often they will also include a **password that you may recognise**. Scary or what!! **Don't be too alarmed**
The password is probably **an old password** (or should be) and they got it through one of the major internet breaches that have been well reported over the years. Adobe, Yahoo, Dropbox (allegedly) and other major sites have been hacked with many millions of user names and passwords being "stolen" and put up for sale or released generally. Once the breach has been discovered those websites usually force the user to change their password and you are safe again. However, your old password is still known, but no longer a problem. That's how its done. However, its important to remember that if you are using that old password on a different site, it would be best to change it. Its as simple as that, and for most people it is not a problem, just looks bad!

There is a web site that you can go to called https://haveibeenpwned.com/

Swanley Computers Ltd
40 High Street, Swanley, Kent. BR8 8BQ 01322 284435
www.swanleycomputers.com

Conclusion.

As you can see there are a lot of potential problems out there but with good solid anti-virus / Internet Security Software you can remain reasonably safe. The key issue is **not to believe everything you read,** don't click onto messages on websites and be careful.

If you think you are infected or require any advice, please feel free to call us. There is no charge for advice and we are happy to help.

Hope you have found this useful and keep an eye open for our You Tube Help Channel which we hope to launch soon.

Thanks for reading and bye for now

Jeremy Beech

Swanley Computers Ltd

We are soon planning to launch our YouTube channel which will feature videos covering some of the above, as well as other useful hints and tips. Visit our website at **www.swanleycomputers.com** where we shall place a link to our channel within the next month.

Thanks.