BeTECHSavvy
Securing Your Digital World

NATIONAL TRADING STANDARDS
Scams Team

How to empower yourself to take a stand against scams & frauds

Take these steps NOW

Incorporating Umbrella Consulting

Introduction

This checklist highlights the steps you can take now to keep your digital-self secure and to mitigate the risks of falling prey to the various scams and frauds out there.

Learn to take control of your digital self, in the same way that you would take control over your personal health, or your finances, or your right to vote.

Hi... My name is Ben Hill, the founder of BeTechSavvy and a National Trading Standards Scam Marshal. Having a productive and safe online digital life is important for you and your family to get the most from online experiences.

With the amount of information that we share online, it is important that we retain the ability to define the boundaries of our digital lives. While many people already have their own go-to tips and tricks, for others, identifying a pragmatic approach to digital privacy and security might seem overwhelming.

More than 5 million people a year fall victim to scams in the UK and 84% of Identity fraud in the UK is carried out via different Internet medium. The average cost to a victim is £3000 and 53% of people over 65 have been targeted by scams. Unfortunately though, a recent survey by National Trading Standards shows that only 5% of scams are reported.

I am also able to provide practical support and advice to people who believe that they may be a target... so feel free to speak to me!

Benjamin Hill

CEO & Founder

How can I protect myself online from on Internet Email Scams or online fraud?

1. Ensure that you have good security protection on your computer / laptop or Macintosh. This should include the minimum of a firewall and antivirus products.
2. If you use web-based email (e.g. Yahoo, Google etc), ensure that the Junk Mail option is used as this will filter out a lot of the scam emails. If you receive a mail that you believe to be junk, classify it as a junk email.
3. If you use Outlook or other proprietary email software, ensure that you have adequate spam filtering or additional software to do this.
4. Do not open attachments in emails unless you know where they have been sent from and are expecting them. If you receive and email out of the blue from someone you do know, if possible contact them via a different method (message or text) asking them if they sent the email with attachment. For additional security, it is recommended to download the attachment to the computer / laptop or Macintosh and then scan it with an antivirus product to ensure that there is no malware attached.
5. Also, remember that banks or other financial institutions will ***never*** ask you to provide account or financial information through an email or via a text message. If you receive such an email/text and you are wary, log in directly to your financial provider's online account portal or call them directly.
6. Before clicking on suspicious links, hover your cursor over the link to view the destination URL. If it does not match the financial website you use, do not click.
7. Remember, if it sounds too good to be true, it usually is!

What should I do if I have received a scam email or if I have already paid money to one?

1. You should ignore it, delete it & not pay any money, even if it appears to be an email of extortion.
2. You should not have any further contact with them. It might be tempting to enter a dialogue with these people, however you should not. These people are professional criminals, they will seek to exploit you. Even if you do not pay them any money, they might seek to steal or abuse your identity. Your best defence against these people is to ignore them and delete any emails that you have received from them.
3. You should report the matter to the Police Authorities, who will investigate your complaint.
4. This is an international crime – investigations must be progressed through the local Police and then Interpol if the scammers are based abroad.
5. The UK police cannot become involved until they have been contacted by Interpol (if based abroad).

Where can I go for advice on Internet Email Scams or on-line fraud?

Action Fraud

This is the place for you to find out about fraud and is the UK's national fraud reporting centre.

Get Safe Online

A joint initiative between the Government, law enforcement, leading businesses and the public sector. Their aim is to provide computer users and small businesses with free, independent, user-friendly advice that will allow them to use the internet confidently, safely and securely.

Stay Safe Online.org

The National Cyber Security Alliance website giving advice on protecting yourself from online fraud.

Friends against Scams

The National Trading Standard Scam website. They have a lot of information on the numerous different types of scams targeting individuals in the UK and how to prevent them. They also offer the ability to become a Scam Marshal, to help with the fight against scammers or can put you

Other Government portals

Many governments in the developed world understand and appreciate that their citizens are more likely to be at risk of being targeted by scammers. Check with local / central government organisations / departments for further information on how to report scams or gain advice if you have been a target of scammers and fraudsters.

---- Remember ----

"The challenge for capitalism is that the things that breed trust, also breed the environment for fraud"

James Surowiecki