If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or http://www.actionfraud.police.uk
If you would like support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.
September Cyber Scam Update

The counterfeiting identity crisis: why buying fake goods online puts you at risk of fraud

Counterfeit goods websites often give the impression of using security authentication to give the site an air of authenticity. This includes the use of recognised images of reputable companies such as Visa, Mastercard and PayPal.

Additionally, many will also claim to have security software and secure transaction verification in place, again using reputable images such as Verisign and McAfee to give them a false 'trust seal'. These images are usually copied and embedded into the illicit website and the sites themselves will not have been approved by the firms.

The authenticity of these trust seals can be confirmed if the consumer attempts to click on any of them – original seals will direct you to the genuine security company. On counterfeit websites these links will not function, as they have no authorised hyperlink attached and will just be embedded images.

How to identify and avoid counterfeit websites:

- The site will usually have grammatical and spelling mistakes; the people behind these sites will try to deceive you by slightly changing the spelling of a well-known brand or shop in the website address;
- Images and web pages will fail or take a substantial amount of time to load;
- Images will have been copied and are usually edited to fit into certain website templates – the pictures may not look proportionate as they have been stretched or reedited;
- There’s often lots of different fonts on the website and it won’t have a professional finish;
- Hyperlinks to associated content will fail to work;
- Look to see where the trader is based and whether they provide a postal address – just because the web address has ‘uk’ do not assume the seller is based in the UK. If there is no address supplied or there is just a PO Box or email, be wary;
- Only deal with reputable sellers and only use sites you know or ones that have been recommended to you. If you have not bought from the seller before, do your research and check online reviews. People will often turn to forums and blogs to warn others of fake sites;
- Ensure the website address begins ‘https’ at the payment stage – this indicates a secure payment;
- Keep security software and firewalls up-to-date.

MONTHS TOP TIPS

Protect yourself from Viruses and Malware:

- Make sure your computer has a firewall and reputable anti-virus software. Without these, your computer has no defence to block infections.
- Take care downloading files. If you don’t know someone who’s sent you an email with an attachment, or you’re not sure about a website offering a file to download, don’t do it out of curiosity.
- Browse safely on the web. Get to know the risks and use the same level of caution as you would in the real world.

Keep up to date with the latest updates on Community Safety in Warwickshire.

Like us on Facebook: www.facebook.com/SafeinWarwickshire
Follow us on Twitter: @SafeInWarks
Visit our site: www.safeinwarwickshire.com

Top Tips:

- If you receive an unexpected high-value package such as a phone, contact the retailer immediately and arrange for it to be sent back, as the scammer may have attempted to intercept the delivery or will pose as a courier to collect the item.
- Check their credentials and call the company they claim to be representing. If you have any fears, contact the police.
- Identity theft is also on the rise so if you spot any suspicious activity on your account report it to your bank immediately.

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or http://www.actionfraud.police.uk
If you would like support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.