Police Briefing Tuesday 21st February 2012
South Herefordshire & Golden Valley

Good Evening!!

Crime Trends

Between **2am** and **7:45am** on **THURSDAY 16-FEB-2012** Several small bales of hay were stolen from near a property in the Wormelow area, an unknown flatbed type vehicle was used to steal it. Incident number 112-S-160212 refers.

On **TUESDAY 21-FEB-2012** near Harewood End, several chainsaws and a quad bike were nearly taken. The offender(s) were disturbed and made off on foot to an unknown vehicle which was parked a short distance away from the area. Incident number 044-S-210212 refers.

A generator and a chainsaw were stolen from a locked up container near Abbey Dore. This happened between the **8th and 11th** of **FEBRUARY.** Incident reference number is 275-S-110212.

A Bus Shelter has been damaged in Madley, this happened Sometime overnight on **SATURDAY 11th** to **SUNDAY 12th FEBRUARY**. A hole had been smashed into one of the Perspex panels, this has then been enlarged gradually over the weekend. A group of youths were seen in the shelter during this time but it is still unknown if they had any involvement or witnessed someone who was. Incident number 26-N-130212 refers.

A Wood Burner was disconnected and taken from an empty property in Peterchurch. There was no forced entry to the property and it could have happened anytime between **13/01/2012** and **14/02/2012.** Incident number is 160-S-160212.

Between **Midday** on **SATURDAY 18-FEB-2012** and **10am** on **SUNDAY 19-FEB-2012** a solar powered electric fencing unit was stolen from a field near Bredwardine. Incident number is 164-S-210212.

If you have any information on any of the above incidents please call us on 101 (our non emergency number) and quote the incident number.

Love Your Computer

Many of you have told us that your worried about your computer's security when using the internet so here is our 10 simple tips to dramatically improve your chances of keeping your information secure and your computer safe from viruses.

1. Always install a good anti-virus programme. Don't run free online scans or download free security software unless you are sure of its origins - some are themselves scams and can install spyware onto your hard drive while others are simply fakes, designed to make you think you are protected even when you're not. Do a web search to check that the software is genuine or buy from a reputable vendor. Make sure the security programme offers real-time scanning - some only check for viruses already present on your computer. Much better to prevent than cure!

2. Keep your software up to date. As well as making sure your anti-virus software has the latest virus definitions files, keep your operating system (e.g. Windows/Mac OS) updated so that it has the latest security patches installed. This way you are making sure that any new or reported vulnerabilities which could allow hackers or criminals access to your computer have been fixed.

3. Switch on your firewall. Firewalls block any unwanted inbound or outbound connections to your computer. You can either use a firewall supplied with your operating system (Windows Firewall, for example, is built into Windows XP, Vista and Windows 7) or third party software. Many anti-virus programmes come with their own firewall, for example.

4. Keep your browser updated. Whether you use Internet Explorer, Firefox, Safari, Google Chrome, Opera or another browser to access the web, make sure you keep it updated to the latest version (often this can be set to happen automatically). Developers are constantly updating these products to protect against any new security vulnerabilities as they are discovered.

5. Secure your Wi-Fi connection. If you connect to the internet using Wi-Fi, make sure you have put in place proper security measures to stop someone from connecting to your network without your permission - otherwise they could run up a large bill which you would responsible for paying. An unsecured Wi-Fi connection can even be used to gain access to your computer remotely. To combat this, make sure you use WPA or WPA2 encryption on your Wi-Fi connections and password protect your broadband router. Also consider using MAC filtering - this will only allow computers and devices you are aware of to connect to your router. Your broadband provider should have information to help you do this.

6. Back up your data. Set up daily or weekly backups of your data to an external or USB drive - that way if you should find yourself 'locked out' from your computer by a virus, you'll still have all your files and information. Equally, use the built in backup features of your operating system (by setting Windows Restore Points, for example) so that if you have problems, you may be able to revert back to a stable system.

7. Be wary of emails that come with attachments and spam emails. Even if the sender is known to you, be wary of opening attachments and always scan them for viruses before opening. Ignore spam emails and don't click the links in them - they could well be to sites with viruses that download when you visit them. And don't reply to spam - this only serves to let the sender know your email address is real!

8. Choose secure passwords. Don't use names of relatives, birth dates or anything else that can easily be guessed. Pick an effective password and use different ones for each website or service you sign up to.

9. Be careful about posting personal information online. It's amazing the amount of detail about ourselves we can reveal online - and can provide rich pickings for the unscrupulous cyber-criminal. Think carefully about the privacy settings you have - especially for social networking sites like Facebook and Google+ - and make sure the information you show online is only seen online by the people you want to see it.

10. Make secure online transactions. If you are buying online or making any other transaction over the internet, make sure you are doing so via a secure connection. Secure websites use special encryption to help keep data such as credit card information secure while it is transmitted over the internet, so only use sites that have a web address beginning with https:// and you can see the padlock symbol in the browser bar.

I hope this helps safe surfing!!

CSO 6482 Kate MIDDLETON
Contact details
Golden Valley & Hereford Rural South Local Policing Teams
PS 3236 Dave Boote dave.boote@westmercia.pnn.police.uk
PC 2368 Chris Lea 07855 785080
PC 2176 Wendy Powell 07811 131525
CSO 6173 Fiona Witcher 07779 141232
CSO 6366 James Cooke 07779 141223
CSO 6482 Katie Middleton 07779 141223
E-mail - goldenvalley.lpt@westmercia.pnn.police.uk