Stroud High School
Headteacher:
Mr Mark McShane BA (Hons)

Registered Office:
Beards Lane
Cainscross Road
Stroud, Glos
GL5 4HF

Telephone: 01453 764441
Fax: 01453 756304
Email: admin@stroudhigh.gloucs.sch.uk
Website: www.stroudhigh.gloucs.sch.uk
Twitter: @stroudhigh

March 2016

Dear Parents/Carers

Gloucestershire Constabulary - Force Safer Cyber Advice Unit, Specialist Crime Division

We have signed up to receive regular updates from Gloucestershire Constabulary regarding cyber-crime advice and warnings. Whilst I promise not to bombard you with information that is not relevant, I will pass on any information about issues that might directly affect you or your families.

On the following page you will see information about phishing and the increase in cyber-fraud which I hope you will find useful, this is also being sent to all staff and students. Please do talk to your children about this, young people are particularly prone to falling foul of clever fraudsters, especially if the communication appears to be 'official', and with the increase in online shopping and banking, this is becoming a real problem.

Kind regards

Mrs Cindi Pride
Deputy Headteacher

Action Fraud reveals that it receives 8,000 reports of phishing scams every month

New data released by Action Fraud and the National Fraud Intelligence Bureau which are both run by the City of London Police , shows that increasingly fraudsters are using phishing as a means to defraud people across the UK. Last year (January 2015 – December 2015), the fraud and cybercrime reporting centre received on average 8,000 reports per month, with 96,699 people reporting that they had received a phishing scam.

Phishing is the attempt to acquire sensitive information, for example usernames, passwords and credit card details or steal money by masquerading as a trustworthy entity in an electronic communication such as email, pop-up message, phone call or text message.

More than 68 percent of people who reported a phishing scam said that they received it in the form of an email, this compares to 12.5 percent of people who said they were contacted by phone, 8.9 percent of people who said that they received a text message and the rest saying they were contacted in another way.

Fraudsters use phishing as means to hook victims into their scams and they are well practiced in making these as convincing as possible. According to a recent report by Verizon , it takes cyber criminals just 82 seconds to ensnare the average victim in a phishing scam and in most cases 23 percent of people will open a phishing email.

In the month of December, the most common phishing scam purported to be either from a bank or from HMRC followed by online payment merchants and utility companies.

In one month, 31 percent of all phishing scams reported to Action Fraud contained a potentially malicious hyperlink, which upon clicking could install malware onto the victim's computer or phone or trick them into providing sensitive information.

Analysis of reports made to Action Fraud reveals that phishing emails used specific subject headings as a means to ensure that the reader would feel compelled to open them. The most common message title for phishing emails is 'Attention' followed by other titles such as 'Your account has been revoked', 'Hello' and 'Important Notification'.

The top email addresses that people reported to have received emails from were; Do-Not-reply@amazon.co.uk, bt.athome@ecomm.bt.com and PQ8MPY@m.apple.com.

Deputy Head of Action Fraud, Steve Proffitt said: "The new figures show that phishing is a problem which is not going away; it is a means for fraudsters to test the water with potential victims and see how many people they can hook into a scam. For the fraudsters, it is a low risk way of casting out their net and seeing what they can catch. If their emails are convincing enough they can yield high returns and people can easily be persuaded into parting with money or to click on links which then infect their computer with malicious software.

"In order to avoid becoming a victim we urge people to be cautious when opening emails and ask them to follow our protection advice in order to make it as difficult as possible for fraudsters who are simply casting around for their next victim".

Behaviours that put you at risk:

- Opening attachments, or clinking on links within emails that are unsolicited or unexpected.
- Responding to emails that ask for your personal or financial details.
- Logging in to a webpage that you have arrived at via a link in an email.

How to protect yourself:

- Don't open attachments or click on the links within any unsolicited emails you receive, and never respond to emails that ask for your personal or financial details. Remember, you can hover over a link to see where it will really take you.
- An email address can be spoofed, so even if the email appears to be from a person or a company you know of, but the message is unexpected or unusual then contact the sender directly via another method to confirm that they sent you the email.
- If you receive an email which asks you to login to an online account, for example due to suspicious activity on your account, instead of clicking on the link provided in the email, go directly to the website yourself.

Mark Godsland. MSyl. Ad Cert Ed&Cp
Force Safer Cyber Advisor
Specialist Crime
Gloucestershire Constabulary