FRAUD FACTS

Fraud Advisory Panel

Issue 3 (revised) December 2012

INFORMATION FOR INDIVIDUALS

Email and internet scams

With most people now regularly accessing the internet and email by computer, tablet or smartphone, the threat from cybercrime is ever present. But what can you do to protect yourself online? This factsheet highlights some of the most common internet and email scams that people can fall victim to.

What is cybercrime?

The term 'cybercrime' encompasses a variety of criminal activity that is committed using a computer, a network or the internet.

It includes computer hacking, virus attacks (eg, 'botnets' and 'malware'), fake websites, cyber-stalking, email scams, and cyber-extortion, to name a few. Often these activities are designed to steal a victim's personal or financial details, or user credentials, for use in fraudulent activities, or to use their computer in an attack on someone else.

Malware

Malware is malicious computer software designed to damage or disrupt a computer system or network. It includes spyware, Trojans, adware and browser hijackers. Some malware is nothing more than a nuisance (eg, pop-up ads), other malware can result in serious security breaches.

Common types of internet and email scams

Internet and email scams are numerous, varied and ever-evolving.

Scams can sometimes be seasonal (such as holiday or Christmas shopping scams), event driven (such as fake charity appeals following natural disasters) or targeted at particular groups of people (such as students starting university). It is important to be aware of the common scams so you can spot and avoid them.

Email

Advance fee frauds (sometimes called 'West African 419' frauds): you receive an unsolicited email from a person who claims to have access to a large amount of money (usually millions) and needs your assistance (and your bank account) to move the money in return for a percentage of the cash. The fraudster will often tell an extraordinary story involving poverty, children and/or lack of education; there are many variations on the theme, but all will urge a quick response and secrecy.

Charity appeal scams: you receive an email appeal for donations purporting to be from a well-known charity usually following a large-scale natural disaster. The email will ask you to make a donation via a link to a fake but credible-looking website. See our separate guidance for donors *Giving Safely*.

Investment scams: you receive an unsolicited email which tries to persuade you to buy a financial product, such as shares, property or other high-value goods, with the prospect of high returns or resale value. See our separate factsheet *Investment Scams* for more information.

Lottery scams: you receive an unsolicited email advising that you have won the lottery, a yacht, a holiday or some other prize – despite never entering a lottery or prize draw. You are asked to pay a small administration fee in order to receive your prize. These scams often originate from overseas.

Phishing scams: you receive an email purportedly from your bank, HMRC, PayPal or a legitimate online business such as a shop or auction website. The email will contain a link to a fake but credible-looking website where you are asked to update your personal and/or account information. Note: banks and other legitimate online businesses will not do this.

Work from home scams (sometimes called 'money mule' or 'money transfer agent' scams): you receive an unsolicited email from a person you do not know who wishes to use your bank account to receive funds. You will then be asked to make a payment to another person or organisation after deducting a percentage as your commission or fee. In some cases the fraudster will lure potential victims through fake job advertisements. Often such scams will try to appeal to university students who are looking for work during 'fresher's week'.

Internet

Game cheats, freeware and file-sharing websites: your computer is infected by a malware virus when you download a game cheat or freeware, or share files online.

Online stores and auctions: you purchase an item online from an e-shop or auction website and either receive an item that does not fit the description or do not receive anything at all. Non-delivery scams are prevalent around Christmas. Sometimes payment is requested by the seller via money transfer companies. More sophisticated high value frauds involve motor vehicle sales in which the buyer is asked to send money by bank transfer to the seller who will offer to deliver the vehicle using a bogus shipping or escrow company. Another variation is where the seller receives a cheque for more than the cost of the vehicle being sold and is then asked by the buyer to return the overpayment with a personal cheque. It will then come to light that the purchaser's cheque is stolen or forged, leaving the seller out of pocket.

Romance fraud and 'honey traps': you are contacted by a person on an online dating site who establishes a rapport with you and then begins to ask to borrow money – for medical treatment, to visit you, or to help a family member in need. Further requests for money will then be received, leaving you out of pocket.

Scareware: you access a website and receive a 'pop-up' telling you that you have some or all of the following: spyware, malware, virus, a Trojan, or pornography downloaded onto your computer. This may be accompanied by a barrage of other pop-ups. You are then offered the chance to purchase a program that can remove all of the above.

Social networking: you post personal information on your profile page, which is then used by cybercriminals to commit identity fraud. Alternatively you download an app which is infected by a virus. See our separate factsheet *Social Networks* for more information.

How to report scams

Action Fraud: if you think you have been the victim of an online scam report it to the national fraud and internet crime reporting centre, www.actionfraud.police.uk.

Citizens Advice consumer service: if you have a dispute about a purchase made online from a UK-based company report it to Citizens Advice, www.citizensadvice.org.uk.

Your financial institution: if you have disclosed your credit or debit card or bank account information as a result of a scam report it to your financial institution.

How to protect yourself

Be aware of the risk from cybercrime and safeguard your computer and personal information while online. There are some simple rules you can follow to reduce the risk of becoming a victim of cybercrime.

DO:

- ✔ Keep security software (such as anti-virus and anti-spyware) and firewalls on your computer, tablet and smartphone up to date – regardless of make or model.
- ✔ Regularly update all your programs with the latest patches.
- ✔ Regularly back up your electronic files so that if anything does go wrong you will not lose everything.
- ✔ Be wary of unsolicited emails from online businesses that you do not know or that offer you investments with unusually high returns.
- ✔ Use different passwords for different accounts. Make sure you choose strong passwords (using a combination of letters, numbers and other characters).
- ✔ Exercise caution when using internet auction websites and always use their preferred payment methods to purchase items.
- ✔ When entering personal or payment information online, check that you are using a secure website. The address should begin 'https' (not 'http') and the padlock symbol should appear in the address bar or the bottom right-hand corner of your browser.
- ✔ Limit the amount of information (especially personal) that you post online or on Twitter.
- ✔ Delete (without opening) unsolicited emails asking you to update your personal and/or account information.
- ✔ Update your internet browser and operating system software as and when a new patch is released.
- ✔ Learn how to encrypt files and documents, particularly when using wireless networks.
- ✔ Permanently delete all of your data from unwanted computers, tablets or smartphones before you get rid of them. You will need to use specialist software to do this properly. Visit Bank Safe Online for useful tips on how to wipe your hard drive.
- ✔ Be careful when downloading game cheats from websites. Only use reputable sites.
- ✔ Check that a website address is genuine by looking for minor spelling differences in the address bar.
- ✔ Regularly review and remove unwanted cookies from your computer.

DO NOT:

- ✗ Respond to unsolicited emails from people or businesses you do not know. Delete them.
- ✗ Access websites via links embedded in emails. Type the website address into the browser yourself.
- ✗ Divulge personal or financial information and passwords to anyone requesting them by email.
- ✗ Use the same password for all of your accounts and sites.
- ✗ Use 'easy' passwords (such as any word from any dictionary).
- ✗ Pay for online purchases using money transfer services.
- ✗ Be fooled by messages in the subject line: 'security notice', 'you're a winner', 'DHL tracking number', 'order confirmation', 'free' anything, 'final notice', 'account closing'.
- ✗ Use web viewers or downloads without reading the terms and conditions of use.
- ✗ Engage in financial transactions that sound too good to be true.

Further information

See our separate fraud factsheets on *Online Shopping Scams*, *Social Networks* and *Wireless Safety* for more information.

Anti-Phishing Working Group
www.antiphishing.org

Bank Safe Online
www.banksafeonline.org.uk

Fraud Advisory Panel
www.fraudadvisorypanel.org

Get Safe Online
www.getsafeonline.org

Knowthenet
www.knowthenet.org.uk

Metropolitan Police Service (Fraud Alert)
www.met.police.uk/fraudalert

Miller Smiles
www.millersmiles.co.uk

The Fraud Advisory Panel gratefully acknowledges the contribution of Tim Harvey (Association of Certified Fraud Examiners) and Mia Campbell in the preparation of this Fraud Fact Sheet.

Fraud Advisory Panel, Chartered Accountants' Hall, Moorgate Place, London EC2R 6EA.
Tel: 020 7920 8721, Fax: 020 7920 8545, Email: info@fraudadvisorypanel.org.
Company Limited by Guarantee Registered in England and Wales No. 04327390
Registered Charity No. 1108863

Distributed by