# SPAM

Managing Unwanted Emails

# Welcome

- Who am I?
  - Jonathan A Burt BSc Cert Mgmt HND FIAP IEng MBCS CITP
    - Batchelor of Science Degree (Open)
    - Professional Certificate in Management
    - Higher National Diploma in Computing
    - Fellow of the Institute of Analysts and Programmers
    - Incorporated Engineer with the Engineering Council
    - Member of the British Computer Society
    - Charted IT Professional
    - PRINCE2 Practitioner
    - Foundation Certificate in IT Service Management (ITIL)
    - Certified Novell Administrator (v5.x)
  - 25+ years experience of working in IT, now retired.
  - Long time member of the Isle of Wight PC User Group!


# Important!

- I cannot guarantee that all of the programs discussed are safe, and they are used at your own risk.  I recommend that you investigate options based on your needs before using any software.
- Always have backups of important data.
- Don’t do anything illegal! ☺

# What is it?

- Spam (stylized as SPAM) is a brand of canned cooked pork made by Hormel Foods Corporation. It was introduced by Hormel in 1937 and gained popularity worldwide after its use during World War II. By 2003, Spam was sold in 41 countries on six continents and trademarked in over 100 countries (excluding the Middle East and North Africa because it is haram and non-kosher).

- Spam's basic ingredients are pork with ham added, salt, water, modified potato starch (as a binder), sugar, and sodium nitrite (as a preservative). Natural gelatin is formed during cooking in its tins on the production line. Many have raised concerns over Spam's nutritional attributes, in large part due to its high content of fat, sodium, and preservatives.

- It has become the subject of a number of appearances in pop culture, notably a Monty Python sketch, which repeated the name many times, leading to its name being borrowed for unsolicited electronic messages, especially email.

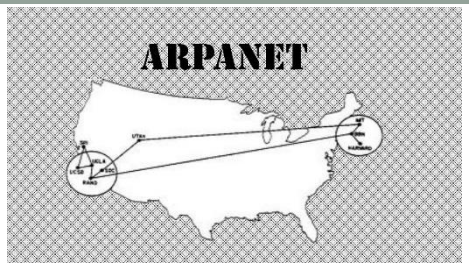
# Questions?

Does anyone have any questions?

# Email Spam

- Email spam, also referred to as junk email, is unsolicited messages sent in bulk by email (spamming).
- The name comes from a Monty Python sketch in which the name of the canned pork product Spam is ubiquitous, unavoidable, and repetitive. Email spam has steadily grown since the early 1990s, and by 2014 was estimated to account for around 90% of total email traffic.
- Since the expense of the spam is borne mostly by the recipient, it is effectively postage due advertising.
- The legal definition and status of spam varies from one jurisdiction to another, but nowhere have laws and lawsuits been particularly successful in stemming spam.
- Most email spam messages are commercial in nature. Whether commercial or not, many are not only annoying, but also dangerous because they may contain links that lead to phishing web sites or sites that are hosting malware or include malware as file attachments.
- Spammers collect email addresses from chat rooms, websites, customer lists, newsgroups, and viruses that harvest users' address books. These collected email addresses are sometimes also sold to other spammers.

# Background




- At the beginning of the Internet (the ARPANET), sending of commercial email was prohibited.
  - Gary Thuerk sent the first email spam message in 1978 to 600 people. He was reprimanded and told not to do it again.
  - Now the ban on spam is enforced by the Terms of Service/Acceptable Use Policy (ToS/AUP) of internet service providers (ISPs) and peer pressure.

- Spam is sent by both reputable organisations and lesser companies. When spam is sent by reputable companies it is sometimes referred to as Mainsleaze.
  - Mainsleaze makes up approximately 3% of the spam sent over the internet.
  - The problem with mainsleaze is that it is generally mixed in with mail that the recipients asked for, and it is difficult to tell the difference using traditional mail filters.
  - As a result, if a mail system filters out all the mail from a mainsleazer, they will get complaints from the people who signed up.

# Background

- It was estimated in 2009 that spam cost businesses around US$130 billion.
- As the scale of the spam problem has grown, ISPs and the public have turned to government for relief from spam, which has failed to materialise.
- Many spam emails contain URLs to a website or websites.
- According to a Cyberoam report in 2014, there are an average of 54 billion spam messages sent every day.

# Spam Techniques

- Phishing
- Appending
- Image Spam
- Blank Spam
- Backscatter Spam
- Virus Loaded

- Fun(?) Fact:
  - In 2004, Jef Poskanzer, owner of the domain name acme.com, was receiving over one million spam emails per day!

# Phishing

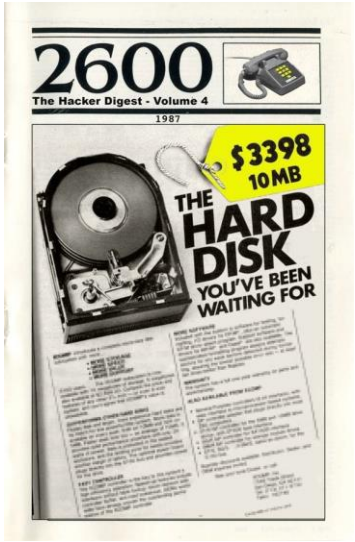
- Spam is also a medium for fraudsters to scam users into entering personal information on fake Web sites using emails forged to look like they are from banks or other organisations, such as PayPal.
- This is known as phishing.
  - Targeted phishing, where known information about the recipient is used to create forged emails, is known as spear-phishing.

# Phishing

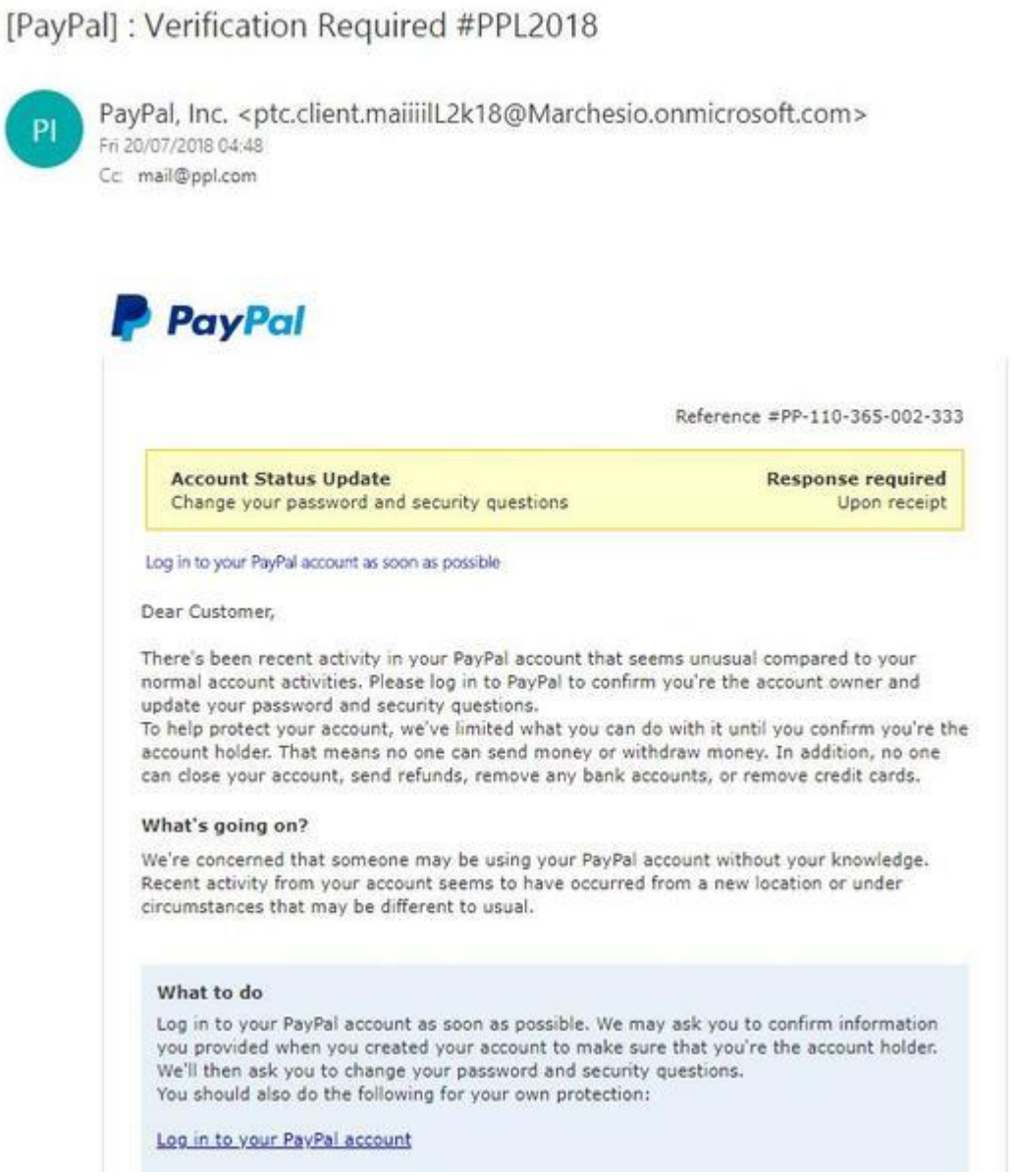
- Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, credit card numbers, or other sensitive details by impersonating oneself as a trustworthy entity in a digital communication.
  - Typically carried out by email spoofing, instant messaging, and text messaging, phishing often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.
- As of 2020, phishing is by far the most common attack performed by cyber-criminals, with the FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime.
  - Attempts to prevent or mitigate the impact of phishing incidents include legislation, user training, public awareness, and technical security measures.

# Phishing

- The first recorded use of the term "phishing" was in the cracking toolkit AOHell created by Koceilah Rekouche in 1995, however it is possible that the term was used before this in a print edition of the hacker magazine 2600.
- The word is a leetspeak variant of fishing (ph is a common replacement for f), probably influenced by phreaking, and alludes to the use of increasingly sophisticated lures to "fish" for users' sensitive information.



# Phishing



[PayPal] : Verification Required #PPL2018

PI

PayPal, Inc. <ptc.client.maiiiilL2k18@Marchesio.onmicrosoft.com>
Fri 20/07/2018 04:48
Cc: mail@ppl.com

PayPal

Reference #PP-110-365-002-333

**Account Status Update**
Change your password and security questions

**Response required**
Upon receipt

Log in to your PayPal account as soon as possible

Dear Customer,

There's been recent activity in your PayPal account that seems unusual compared to your normal account activities. Please log in to PayPal to confirm you're the account owner and update your password and security questions.
To help protect your account, we've limited what you can do with it until you confirm you're the account holder. That means no one can send money or withdraw money. In addition, no one can close your account, send refunds, remove any bank accounts, or remove credit cards.

**What's going on?**

We're concerned that someone may be using your PayPal account without your knowledge. Recent activity from your account seems to have occurred from a new location or under circumstances that may be different to usual.

**What to do**

Log in to your PayPal account as soon as possible. We may ask you to confirm information you provided when you created your account to make sure that you're the account holder. We'll then ask you to change your password and security questions.
You should also do the following for your own protection:

Log in to your PayPal account

benhtieudem.com.vn/lahshish.html

# Appending

- Email appending, also known as e-appending, is a marketing practice that involves taking known customer data (first name, last name, and postal address) and matching it against a vendor's database to obtain email addresses.
  - The purpose is to grow one's email subscriber list with the intent of sending customers information via email instead of through traditional mail.
  - Email appending is a controversial practice in the email marketing world, with critics claiming that sending email to people who never explicitly opted-in is against best practices.

- An email appending process involves either a business or consumer database made up of contacts including their name, address and company name [for business contacts].
  - If the company wants to expand into email communication, then they can involve a service provider that has a database of email addresses in order to merge the data and append business or consumer email addresses to their existing file.
  - In this way they can have an updated database with the current email address of individuals on the list. The success of email appending depends on the quality of both databases being merged.

# Appending

- Like other forms of Database marketing, marketing materials sent using e-pending may be considered spam.
  - Mailers using appending by definition do not have consent of the individuals on their lists, since the individuals did not disclose their email addresses to begin with.
  - Mail sent by appending methods therefore is Opt-out instead of Opt-in e-mail.

- In September 2011, The Messaging Anti-Abuse Working Group (MAAWG) released a position paper stating the practice of email appending is in direct violation to their values and is an abusive practice.

# Image Spam


- Image-based spam, or image spam, is a kind of email spam where the textual spam message is embedded into images, that are then attached to spam emails. Since most of the email clients will display the image file directly to the user, the spam message is conveyed as soon as the email is opened (there is no need to further open the attached image file).

- The goal of image spam is clearly to circumvent the analysis of the email's textual content performed by most spam filters.
  - Accordingly, for the same reason, together with the attached image, often spammers add some "bogus" text to the email, namely, a number of words that are most likely to appear in legitimate emails and not in spam.

# Image Spam


- Consequently, optical character recognition tools were used to extract the text embedded into spam images, which could be then processed together with the text in the email's body by the spam filter, or, more generally, by more sophisticated text categorisation techniques.
  - Further, signatures (e.g., MD5 hashing) were also generated to easily detected and block already known spam images.
  - Spammers in turn reacted by applying some obfuscation techniques to spam images, similarly to CAPTCHAs, both to prevent the embedded text to be read by OCR tools, and to mislead signature-based detection.

- This raised the issue of improving image spam detection using computer vision and pattern recognition techniques.

# Image Spam

- Image spam started in 2004 and peaked at the end of 2006, when over 50% of spam was image spam. In mid-2007, it started declining, and practically disappeared in 2008.
- The reason behind this phenomenon is not easy to understand.
  - The decline of image spam can probably be attributed both to the improvement of the proposed countermeasures (e.g., fast image spam detectors based on visual features), and to the higher requirements in terms of bandwidth of image spam that force spammers to send a smaller amount of spam over a given time interval.
- Both factors might have made image spam less convenient for spammers than other kinds of spam.
- Nevertheless, at the end of 2011 a rebirth of image spam was detected, and image spam reached 8% of all spam traffic, albeit for a small period.

# Blank Spam

- Blank spam is spam lacking a payload advertisement. Often the message body is missing altogether, as well as the subject line. Still, it fits the definition of spam because of its nature as bulk and unsolicited email.
- Blank spam may be originated in different ways, either intentional or unintentionally:
  - Blank spam can have been sent in a directory harvest attack, a form of dictionary attack for gathering valid addresses from an email service provider. Since the goal in such an attack is to use the bounces to separate invalid addresses from the valid ones, spammers may dispense with most elements of the header and the entire message body, and still accomplish their goals.
  - Blank spam may also occur when a spammer forgets or otherwise fails to add the payload when he or she sets up the spam run.
  - Often blank spam headers appear truncated, suggesting that computer glitches, such as software bugs or other may have contributed to this problem—from poorly written spam software to malfunctioning relay servers, or any problems that may truncate header lines from the message body.

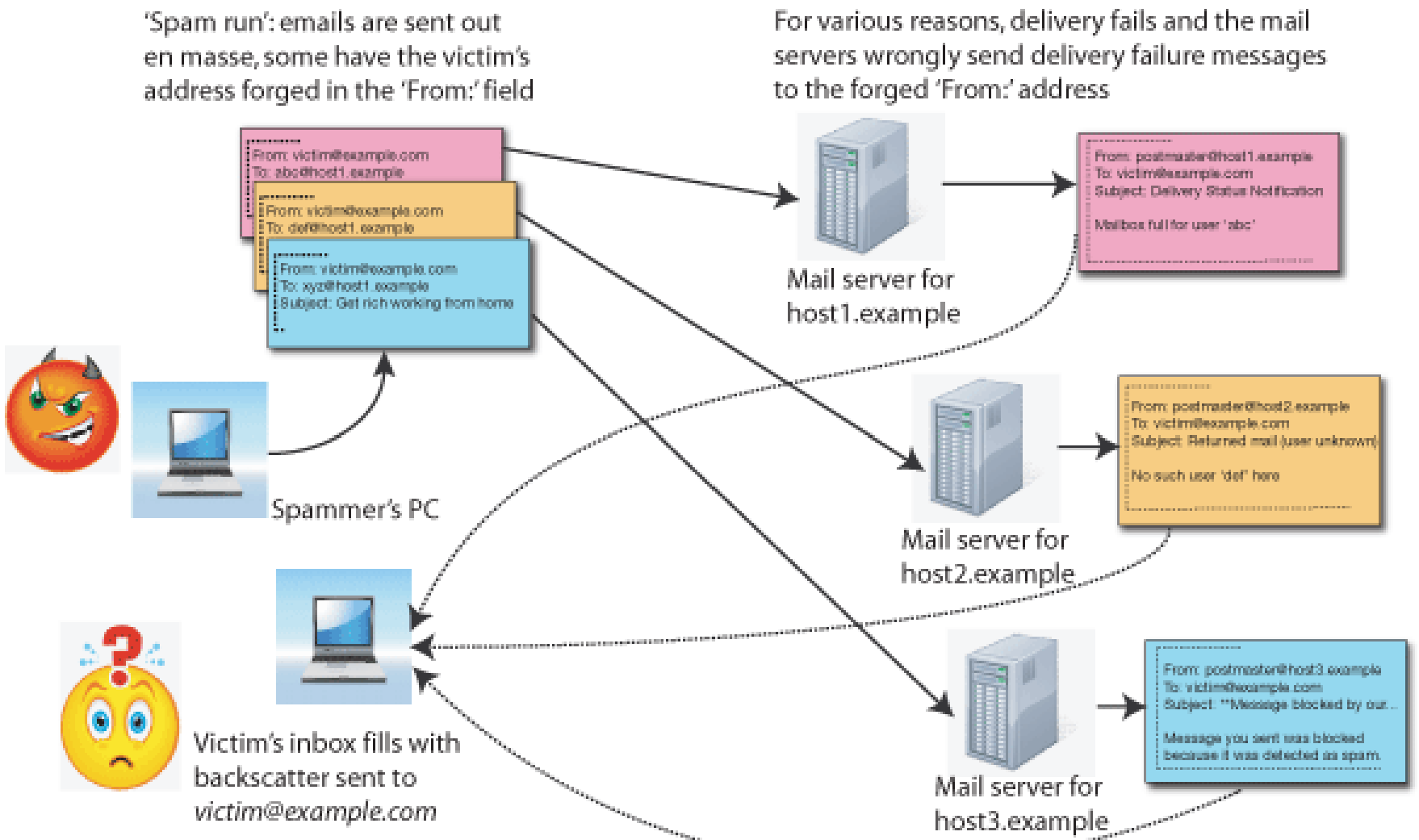
# Backscatter Spam

- Backscatter (also known as outscatter, misdirected bounces, blowback or collateral spam) is incorrectly automated bounce messages sent by mail servers, typically as a side effect of incoming spam.
- Recipients of such messages see them as a form of unsolicited bulk email or spam, because they were not solicited by the recipients, are substantially similar to each other, and are delivered in bulk quantities.
- Systems that generate email backscatter may be listed on various email blacklists and may be in violation of internet service providers' Terms of Service.

# Backscatter Spam

- Backscatter occurs because worms and spam messages often forge their sender addresses.
  - Instead of simply rejecting a spam message, a misconfigured mail server sends a bounce message to such a forged address. This normally happens when a mail server is configured to relay a message to an after-queue processing step, for example, an antivirus scan or spam check, which then fails, and at the time the antivirus scan or spam check is done, the client already has disconnected.
  - In those cases, it is normally not possible to reject the SMTP transaction, since a client would time out while waiting for the antivirus scan or spam check to finish. The best thing to do in this case, is to silently drop (delete) the message, rather than risk creating backscatter.

# Backscatter Spam



# Virus Loaded

- Some spam may appear to be blank when in fact it is not.
- An example of this is the VBS.Davinia.B email worm which propagates through messages that have no subject line and appears blank, when in fact it uses HTML code to download other files.

# Legal Countermeasures

- European Union
  - Article 13 of the European Union Directive on Privacy and Electronic Communications (2002/58/EC) provides that the EU member states shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

- United Kingdom
  - In the United Kingdom, for example, unsolicited emails cannot be sent to an individual subscriber unless prior permission has been obtained or unless there is a pre-existing commercial relationship between the parties.

# How to deal with Spam


- Best practice is to ignore them and delete them.
  - However, if your email client supports it, you can mark it as Junk/Spam, and it will go to a block-list within your email client.
  - If you are using a third-party spam filter, you might be able to mark it as Spam for investigating by the provider to add to their Spam list.
- Phishing
  - Any email which says it comes from PayPal, your Bank, or basically any other legitimate business site which asks you to click on a link to verify your details is generally fake!
  - The only time when it might be legitimate is when **you have** just requested a password reset on the website or just joined a website, and an email comes though for you to click on a reset password link or validate email link.

# Unsubscribe

- If the spam is from a legitimate company, for example B&Q, Amazon, etc. Then they must by law have a section in the email which gives you the option to unsubscribe.
  - This is normally “hidden” at the end of the email.
- Doing this will reduce the amount of emails you get from legitimate companies, but it can take up-to seven days for them to correctly purge your request from their email lists.
- However, if it is a generic spam message from an unknown domain, then do not unsubscribe. As all this does is confirm that your email address is valid and will lead to more Spam!

# Unsubscribe

amazon.co.uk

Connect with us

We hope you enjoyed receiving this message. However, if you'd rather not receive future e-mails of this sort from Amazon.co.uk please opt-out here.

Terms and conditions apply. Click on the offer for details of applicable products and terms and conditions. Offers are for a limited time only and subject to availability. Discounts and savings on offers on products sold by Amazon.co.uk (excluding MP3s) refer to savings against Recommended Retail Price ("RRP") or our previous selling price, as indicated. Discounts and savings on Amazon MP3s refer to savings against our previous selling price, or as otherwise indicated. Offers on products sold by a Marketplace seller are subject to that seller's terms and conditions of sale. See www.amazon.co.uk for details.

Amazon.co.uk is a trading name for Amazon EU Sarl, for Amazon Media EU and for Amazon Services Europe Sarl, all of which have their registered office at 5 Rue Plaetis, L-2338 Luxembourg.

Please note that this promotional e-mail is being sent from an e-mail address that cannot receive e-mails. If you have any questions and wish to contact us, click here.

Amazon Video Limited, a company registered in England and Wales. Registered office: Leadenhall Court, One Leadenhall Street, London, EC3V 1PP, United Kingdom.

# Surveys

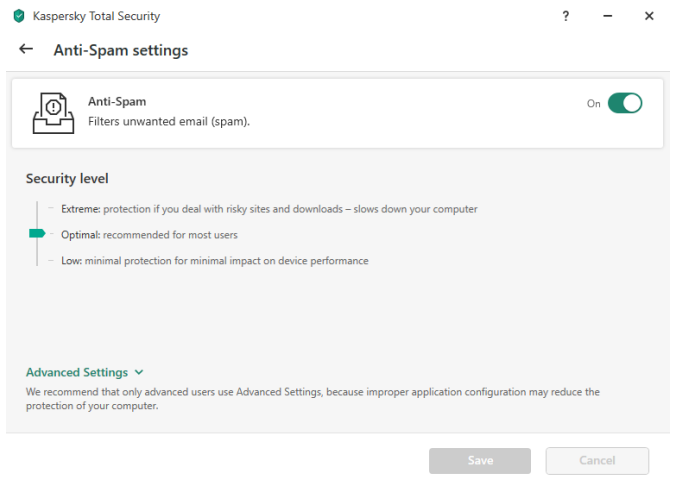
- There are often online surveys which people are asked to complete, perhaps with the option to enter a prize draw.
  - Filling these in is not a good idea, as what the survey is doing is collating valid email addresses along with information of the recipient likes, dislikes, interests etc.
  - This can then be sold on to spammer and companies who do not care about generating Spam (as it's seen as "free advertising").
  - If you do want to fill these in, then have what I call a *throw-away email address*; a different email address from your main one which you use for this purpose only.
    - This way you know the email account is going to receive Spam and can prepare accordingly.

# Throwaway Emails

- Have a *throw-away email address*; a different email address from your main one which you use for this purpose only.
- This can then be use on less secure websites you visit, for example:
  - Forums Registration
  - Online Surveys
  - Mailing Lists
  - Websites for Hobby's, Leisure Activities
- Basically, the more protection you take with where you use your email address and who you share it with will help to reduce your Spam intake!

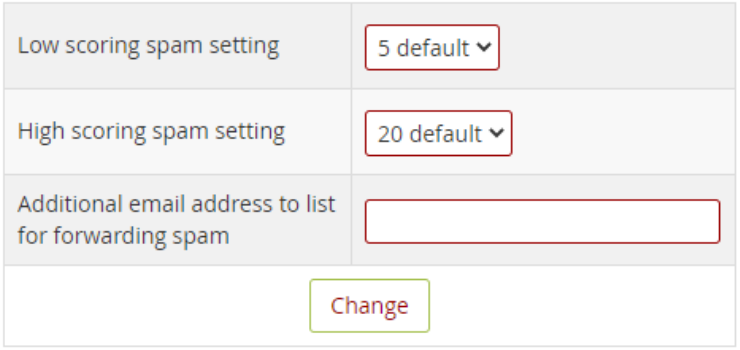
# Internet Security (& Antivirus) Software

- Most paid Internet Security (& Antivirus) software packages, for example, Kaspersky Total Security, have options to mark messages as Spam.
- This doesn't delete the spam, as it reads them as they are downloaded and usually marks the subject line with [SPAM], or something similar. You can then setup a rule in your email client to automatically move emails marked that way to a Spam folder.



# ISP Settings

- If you have your own domain and a private email, like Jonathan@jaburt.com, then the control panel from the hosting company will have options for Spam filtering.
  - HostPresto! use the opensourced MailScanner as their Spam filtering software.




Current Settings

| Domain | Spam Scanning | Low Scoring Spam | High Scoring Spam | Virus Scanning | Deliver Cleaned Emails |
|---|---|---|---|---|---|
| jaburt.com | yes | Deliver | Delete | yes | yes |
| | [1] | [2] | [3] | [4] | [5] |

# Spam-Washing Software

- Spam-Washing software is software that has been specially designed to check your email for Spam, and filter them out, using:
  - a database of known spam messages
  - tools to identify possible new ones

- The benefits of Spam-Washing software is that they check the emails on the email server, and deletes* Spam there.
  - This saves you the hassle of downloading the emails to your email client.
  - Can save you download bandwidth, useful for mobile and ISPs which don’t offer unlimited bandwidth.
  - Generally there is a cost to use this software, however most offer free trials and even free versions (for one email account).

*However, not all free products check on the server and instead rely on your email client downloading the spam first.

# Spam-Washing Software

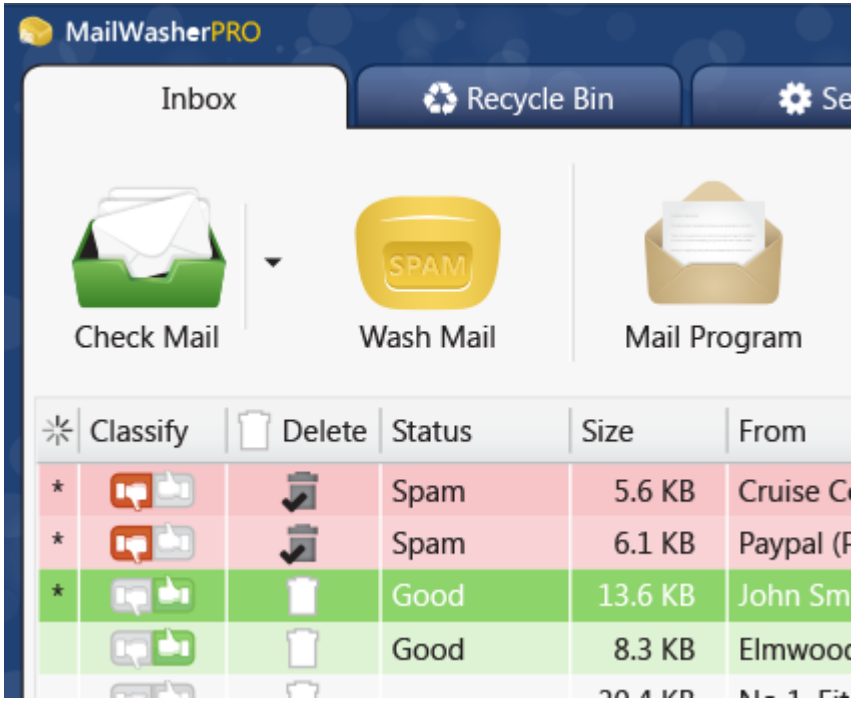
- Here is a short list of some of the software packages available:
  - Mailcleaner (Free)
  - MailScanner (Opensourced)
  - Mailwasher (Free & Paid)
  - MX Guarddog (Free Trail & $0.25/email address/month)
  - POPFile (Free)
  - SpamAssassin (Opensourced)
  - SpamBayes (Opensourced, but not updated in a few years)
  - SpamBully (Free Trail)
  - SPAMfighter (Free & Paid)
  - Spamihilator (Free)

Paid versions are generally on an annual subscription basis.

# MailWasher Free

- Both the paid and free version of MailWasher offer:
  - Preview emails on the server
  - Delete emails at the server
  - Effective anti-spam tools
  - POP3, IMAP, Hotmail, AOL, Gmail etc
  - Colored grid lines for easy reading
  - Real-time spam flter service
  - Auto delete spam
  - Search inbox
  - Automatic updates
  - Customize interface
- However, the free version only support 1 email address, and has access to technical support.

# MailWasher Free



# Questions?

Does anyone have any questions?

# Further Information

- Wikipedia
  - https://en.wikipedia.org/
- Lots of useful tutorials
  - http://www.howtogeek.com/
- TechRadar has a good selection of reviews.
  - http://www.techradar.com/
- LinkedIn
  - https://www.linkedin.com/in/jaburt/