Staying Safe on the Internet

Nigel Callaghan

Director
Technoleg Taliesin Cyf.

Technoleg Taliesin

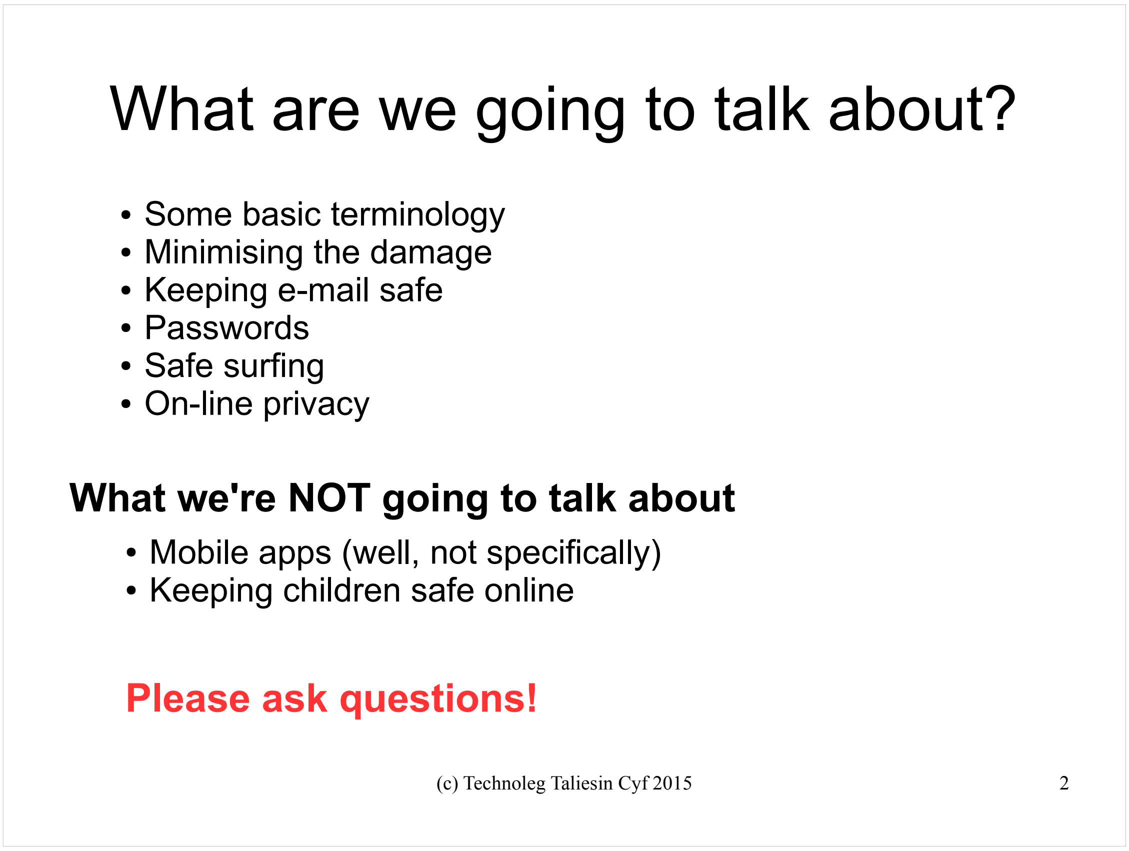
Siop Cynfelyn
@Cletwr

During the next hour we're going to be trying to make your use of the Internet a tiny bit safer. The Internet is a magnificent, mind-boggling invention. Pure science fiction. But It's a dangerous world out there!

Why am I qualified to give this talk?

I've been using the internet since the beginning. I was using e-mail on my Sinclair Spectrum in the mid-eighties. I was surfing the world wide web in 1992 (what little of the web there was). I was writing websites that calculated motor insurance premiums in the late nineties. I registered my first domain in 1998, and built my first website around the same time.

I've watched it grow and develop to be the ubiquitous, essential tool that it is today, and seen how scumbags try to use it to rip people off for fun or profit. That's life...I suppose it's better than being mugged at knife-point!



What are we going to talk about?

- Some basic terminology
- Minimising the damage
- Keeping e-mail safe
- Passwords
- Safe surfing
- On-line privacy

What we're NOT going to talk about

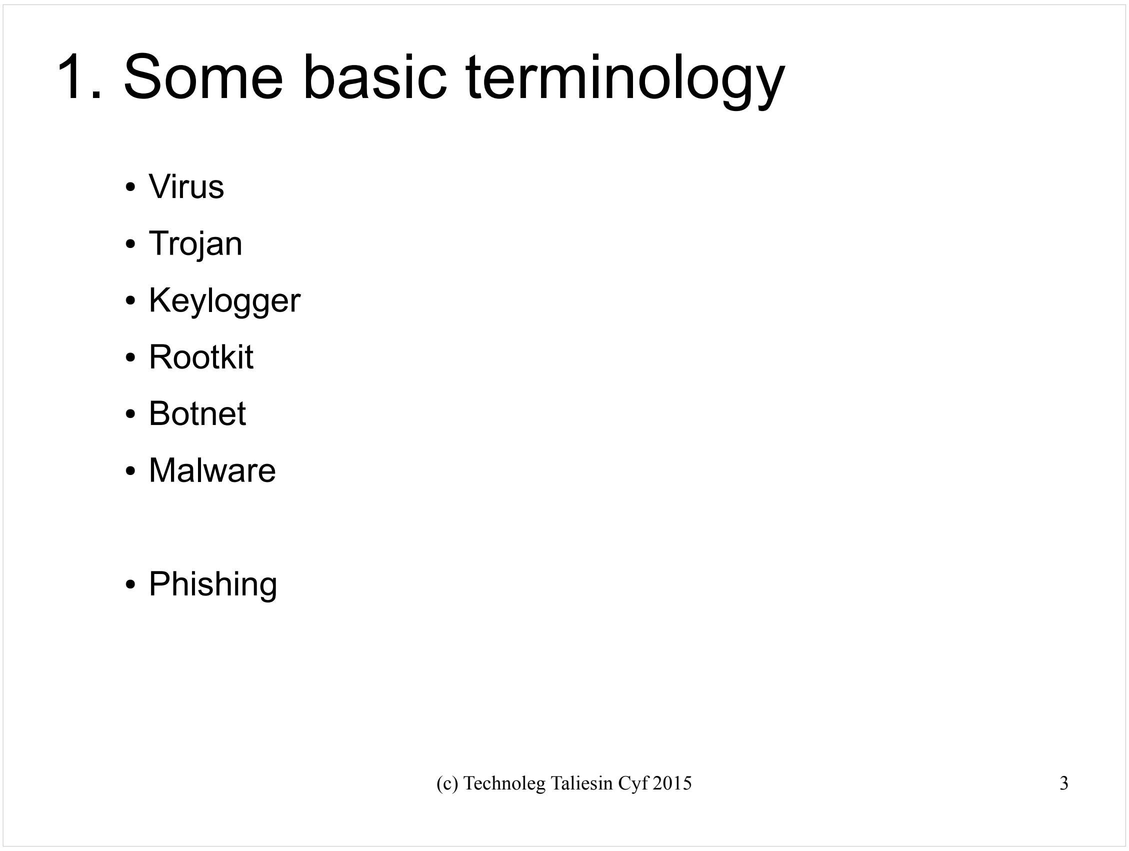
- Mobile apps (well, not specifically)
- Keeping children safe online

Please ask questions!

There's a lot to cover!

Copy of slides is available online

For detailed help, Google is your friend!



1. Some basic terminology

- Virus
- Trojan
- Keylogger
- Rootkit
- Botnet
- Malware

- Phishing

Viruses are programs that masquerade as something else or attach themselves to another program and then spread/act when the program is run. Can also be carried in word docs, spreadsheets, zip files etc.

Trojans look like something good, but do bad things

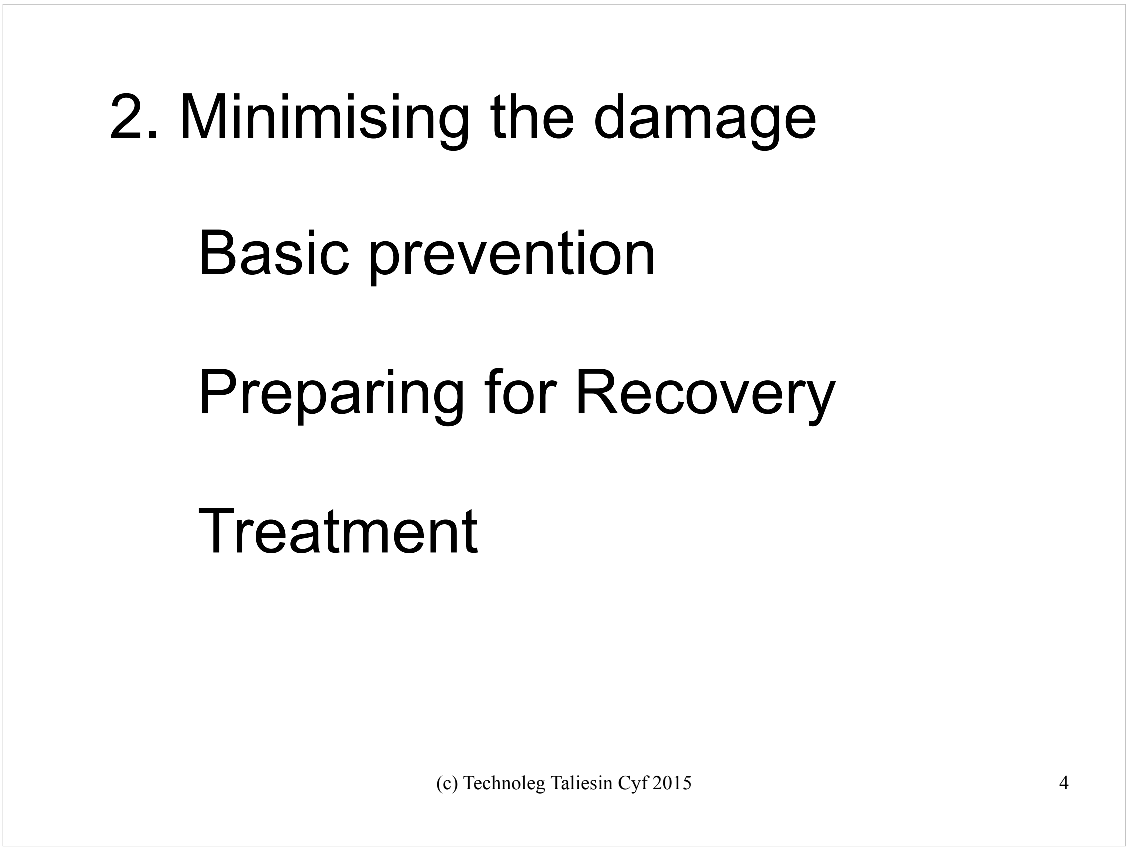
Keyloggers record your keystrokes (passwords?) and send them home

Rootkits get in deep and can do all sorts of bad things – they give total control of your computer to a bad person.

Botnets are networks of computers that have been taken over, often not visible to the owner, and can be used to send spam e-mail, attack websites and worse

Malware is a generic name for all of the above

Phishing is an attempt to collect personal information, passwords etc by faking a website login page etc.



2. Minimising the damage

Basic prevention

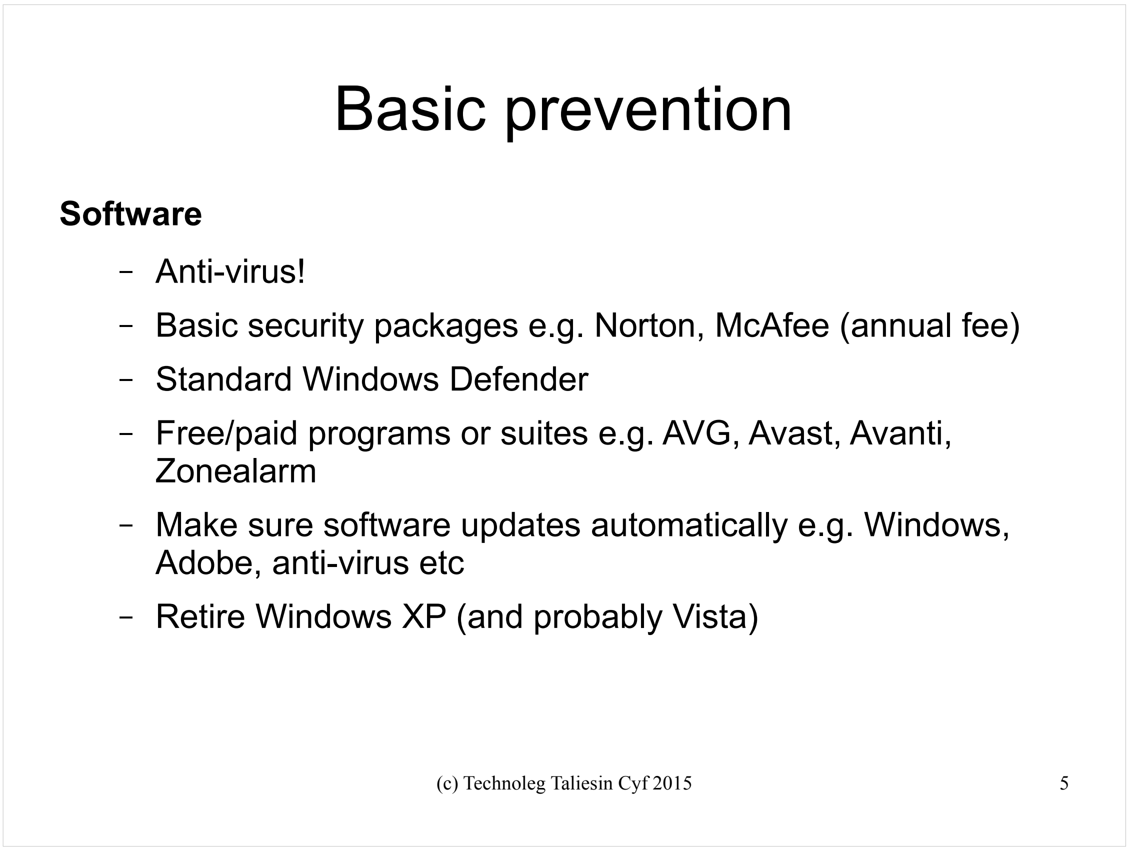
Preparing for Recovery

Treatment

Sadly, I can't tell you how to completely avoid problems. Behind the simplest website is an incredibly complicated system, or set of systems. Your computer runs (usually) Windows, your phone iOS or Android, each of which contains millions of lines of code, and took many thousands of man-years to develop. It's not going to be perfect! Ditto with the programs behind the websites.

The more powerful, useful, flexible and user-friendly we make things, the more opportunities there are for holes that can be exploited by the baddies. And don't get me started on the 'Internet of Things'....

All we can really do is minimise the opportunities they have, but accept that one day they WILL get through the defences, and make sure we can minimise the damage and simplify the recovery process



Basic prevention

Software

- Anti-virus!
- Basic security packages e.g. Norton, McAfee (annual fee)
- Standard Windows Defender
- Free/paid programs or suites e.g. AVG, Avast, Avanti, Zonealarm
- Make sure software updates automatically e.g. Windows, Adobe, anti-virus etc
- Retire Windows XP (and probably Vista)

This covers some of the fundamentals.

Trust nothing! No such thing as a 'safe' site. Even software DVDs have had viruses. An ounce of prevention...(M&S site problem – adverts – Adblock Plus?)

Software: you MUST have appropriate AV and related software.

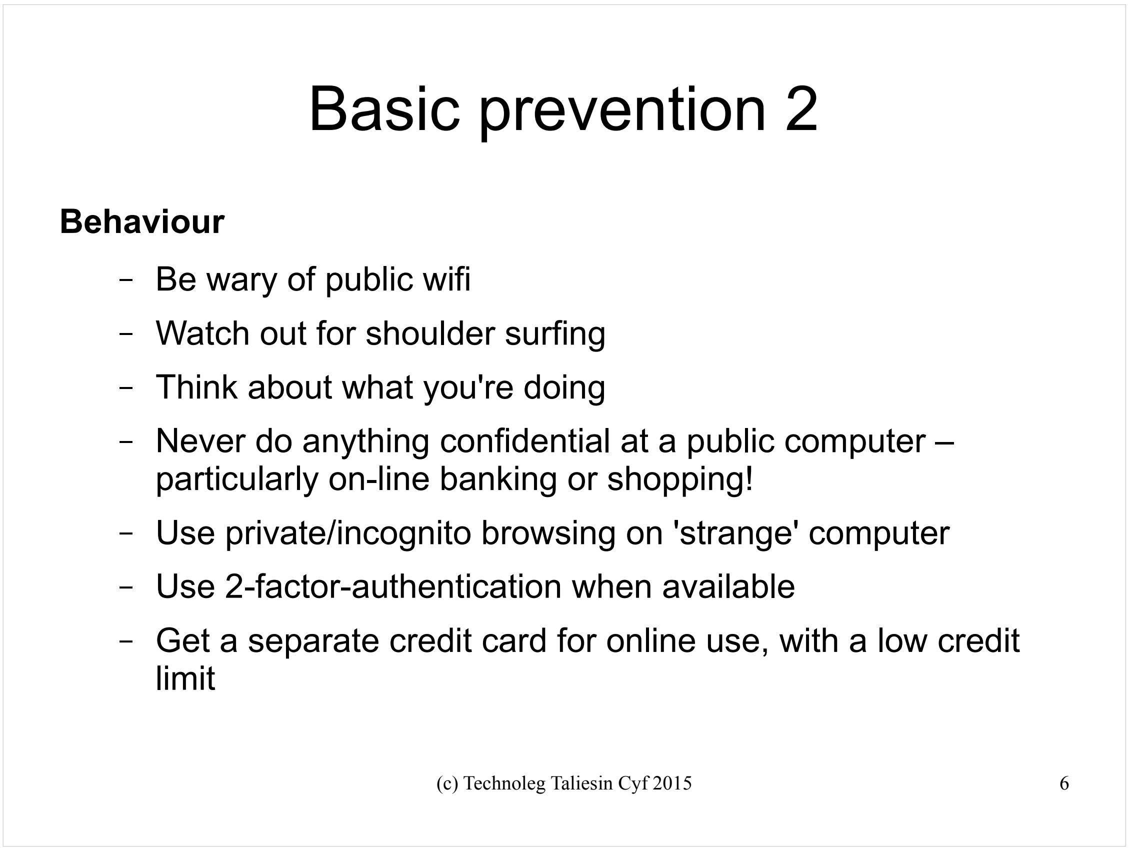
Anti-virus – continuously looks for Viruses. Not 100%

BE CAREFUL WHAT YOU DOWNLOAD! Don't click on the 'Ads' at the top of Google search results, make sure you go to the 'real' site. See links page.

Firewall – stops ET phoning home, and burglars probing your pc.
Tricky to understand firewalls – basically read the message, and if you don't expect it, then say NO!

Often worth paying for paid version of free stuff – nagware is a pain.

Windows XP – no more security updates, Vista ends in 2017.



Basic prevention 2

Behaviour

- Be wary of public wifi
- Watch out for shoulder surfing
- Think about what you're doing
- Never do anything confidential at a public computer – particularly on-line banking or shopping!
- Use private/incognito browsing on 'strange' computer
- Use 2-factor-authentication when available
- Get a separate credit card for online use, with a low credit limit

Public Wifi etc.

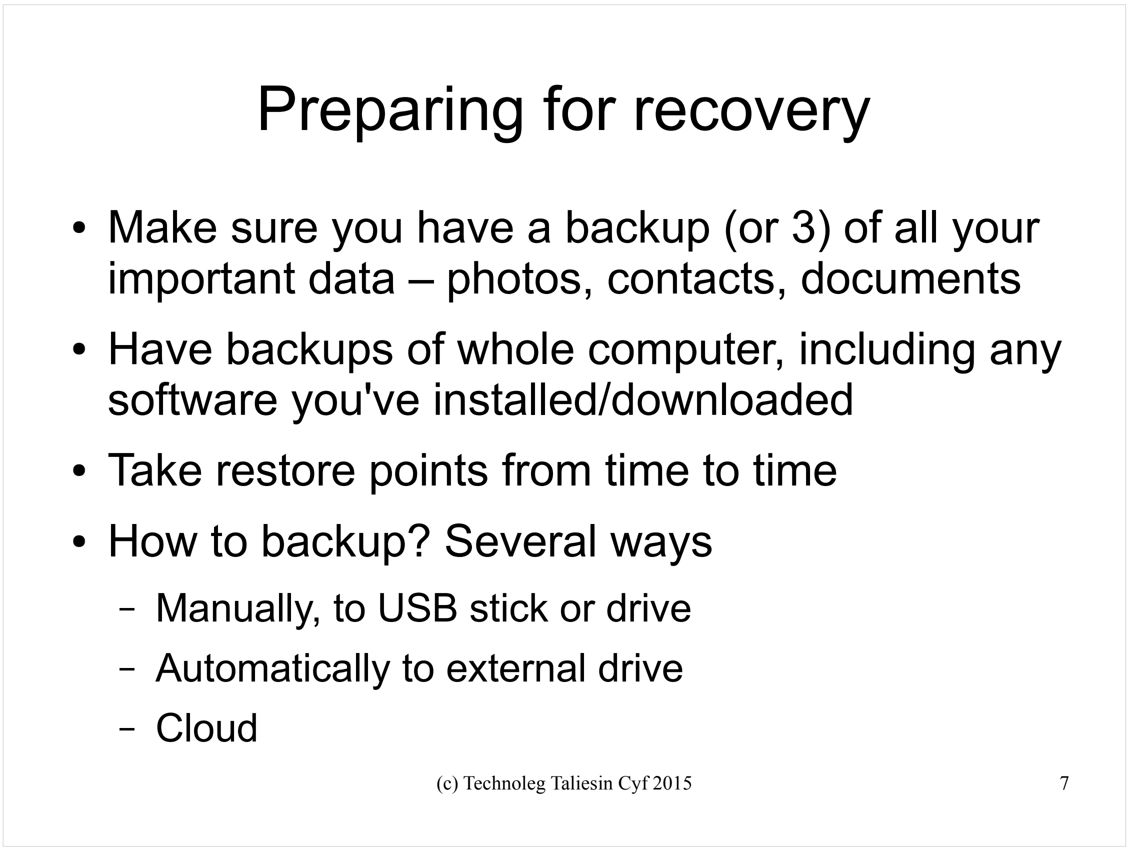
If you're a regular user of public wifi worth thinking about VPN software. (Explain what it is). Has other uses – watching US and Spanish TV, Irish sports etc.

Make sure public WiFi is secure (asks for a password)

Behaviour – think about what websites you're visiting

Private browsing / 2FA – give a demo with Gmail

Trust no-one!



Preparing for recovery

- Make sure you have a backup (or 3) of all your important data – photos, contacts, documents
- Have backups of whole computer, including any software you've installed/downloaded
- Take restore points from time to time
- How to backup? Several ways
  - Manually, to USB stick or drive
  - Automatically to external drive
  - Cloud

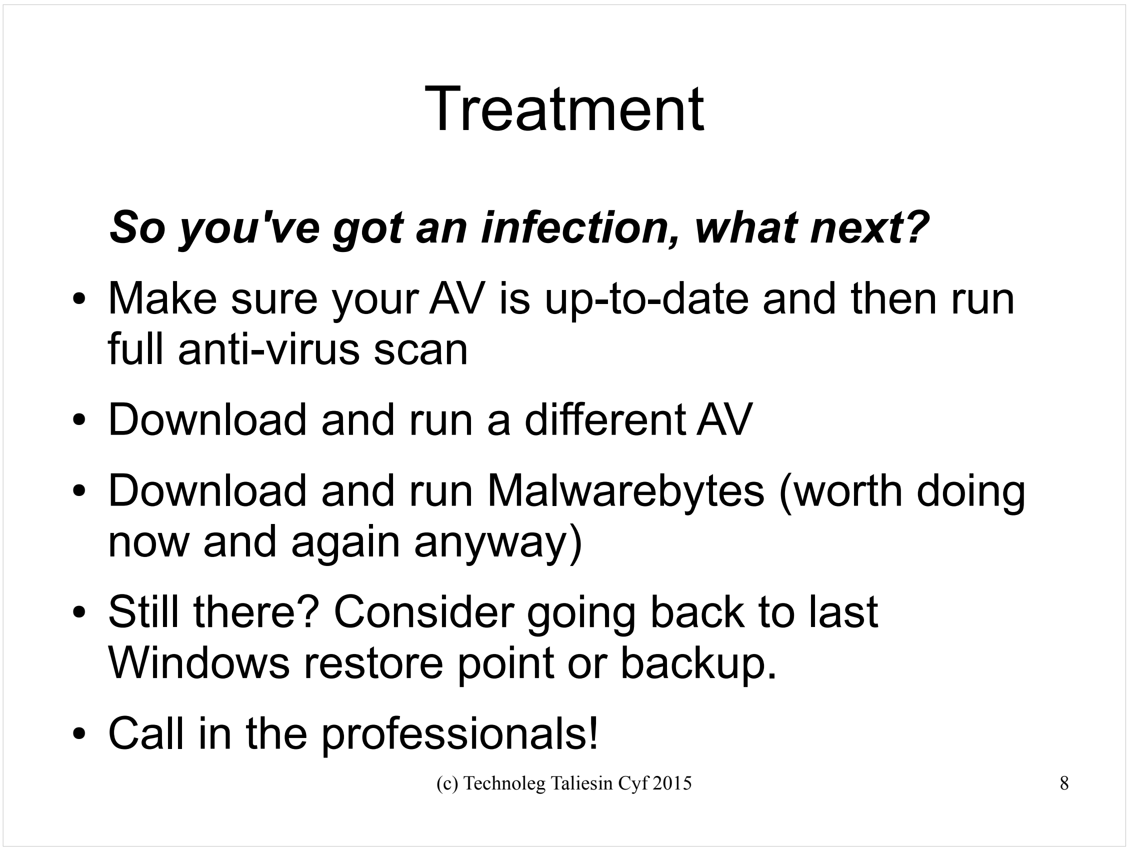
How you backup depends on how paranoid you are and how valuable your data is to you.

Wedding photos? Get them printed! Talk to local camera shop.

What are you protecting against? Obviously viruses and malware, but what about fire and burglars? Some 'off site' backups are handy.

How to backup? Recent versions of windows have software built in, or you can buy some very effective automatic stuff.

What backup drives? They're all pretty cheap (compared to the value of data)
USB – good for data, under £20 for 64GB
External drive – for full drive backup, £40-50 for 1TB
Cloud – Dropbox is 2GB free, £8/month for more, but upload is slow. Would you trust it with something confidential?

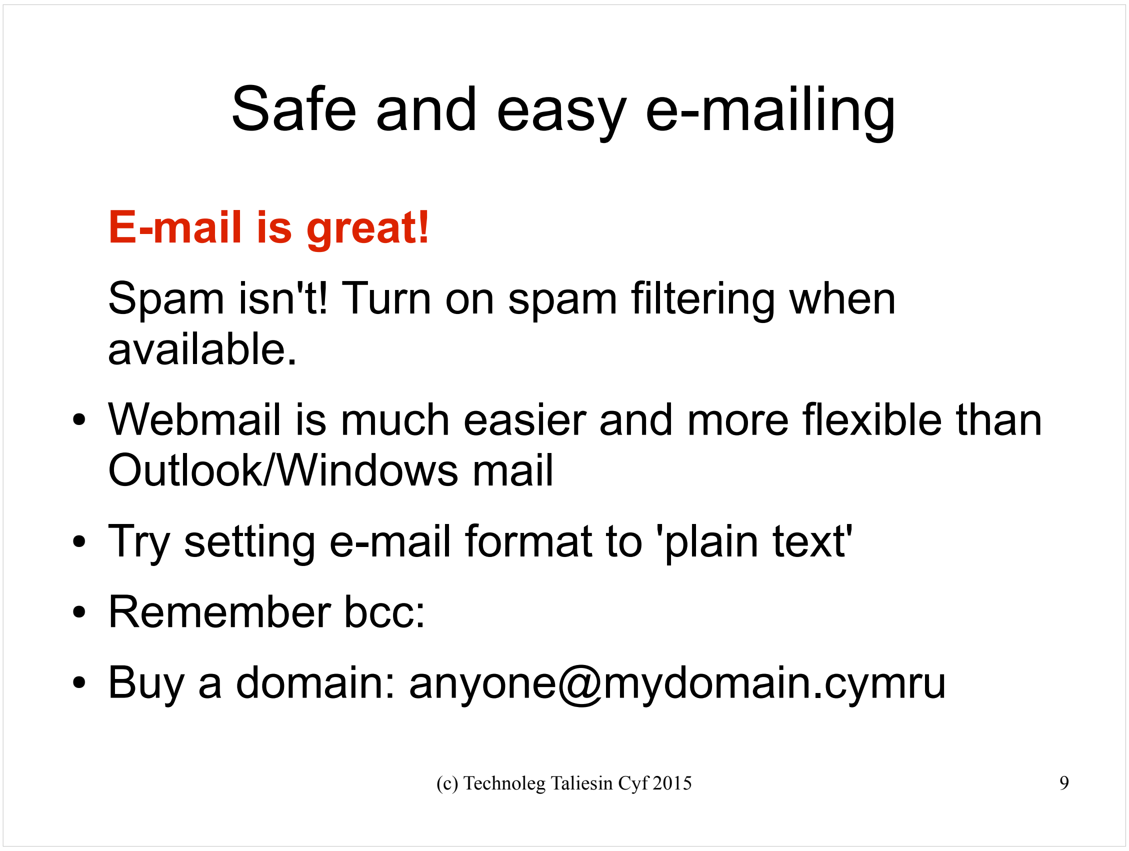


Treatment

So you've got an infection, what next?

- Make sure your AV is up-to-date and then run full anti-virus scan
- Download and run a different AV
- Download and run Malwarebytes (worth doing now and again anyway)
- Still there? Consider going back to last Windows restore point or backup.
- Call in the professionals!

To be honest, Malwarebytes sorts out most things



Safe and easy e-mailing

E-mail is great!

Spam isn't! Turn on spam filtering when available.

- Webmail is much easier and more flexible than Outlook/Windows mail
- Try setting e-mail format to 'plain text'
- Remember bcc:
- Buy a domain: anyone@mydomain.cymru

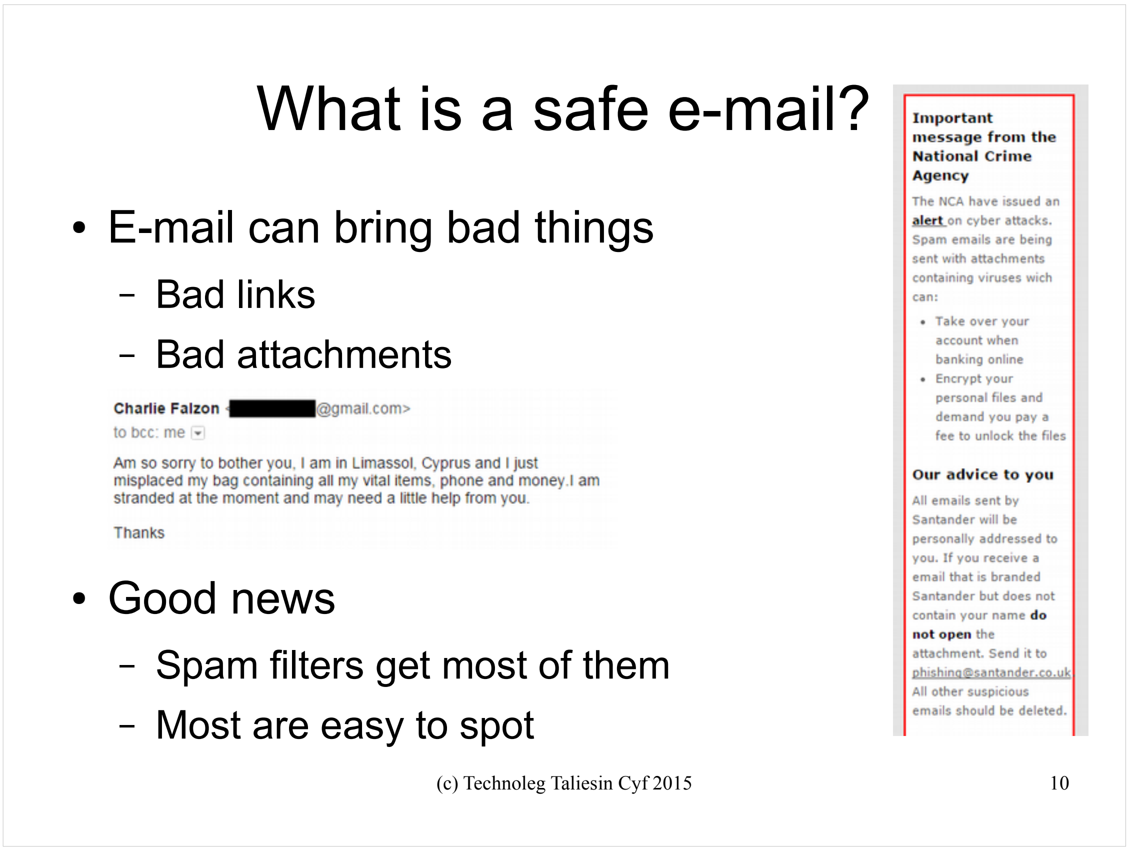
Trust no-one!

Spam filters are useful, but check your spam box from time to time in case of errors. It can be quite entertaining too!

Dodgy e-mails can come from compromised accounts of friends and relatives. “At a conference in Kenya, lost ticket, send money”

Bcc: helps protect your friends privacy.

Own domain with e-mail forwarding means you can easily change ISP and not worry about losing your @btinternet.com address. Can also have multiple addresses



What is a safe e-mail?

- E-mail can bring bad things
  - Bad links
  - Bad attachments

Charlie Falzon [redacted]@gmail.com>
to bcc: me

Am so sorry to bother you, I am in Limassol, Cyprus and I just misplaced my bag containing all my vital items, phone and money.I am stranded at the moment and may need a little help from you.

Thanks

- Good news
  - Spam filters get most of them
  - Most are easy to spot

Important message from the National Crime Agency

The NCA have issued an **alert** on cyber attacks. Spam emails are being sent with attachments containing viruses wich can:

- Take over your account when banking online
- Encrypt your personal files and demand you pay a fee to unlock the files

Our advice to you

All emails sent by Santander will be personally addressed to you. If you receive a email that is branded Santander but does not contain your name **do not open** the attachment. Send it to phishing@santander.co.uk All other suspicious emails should be deleted.

Don't follow links from e-mails, even if it's from someone you know. Their account could have been hi-jacked, as in the example here.

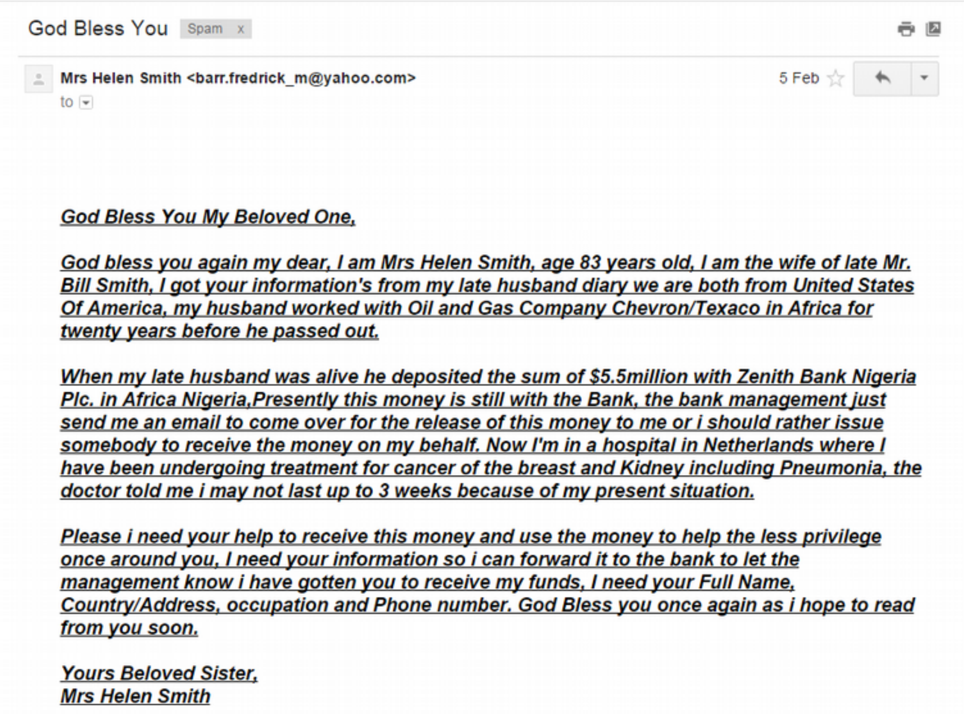
Note: incoming e-mail addresses can easily be faked

There are a lot of warning signs: bad english, odd/unlikely e-mail addresses, addressed to 'Dear Customer', Dear User, Dear Friend – real businesses (banks etc) address you by name and usually include some sort of account number.

Many real businesses, particularly banks, will not send important messages by e-mail, and will not include links.

If you do get an e-mail that looks like it's from your bank, DON'T follow the links. Go to a bookmark in your browser and log in from there.

Let's look at some examples...



God Bless You

Mrs Helen Smith <barr.fredrick_m@yahoo.com>
to

God Bless You My Beloved One,

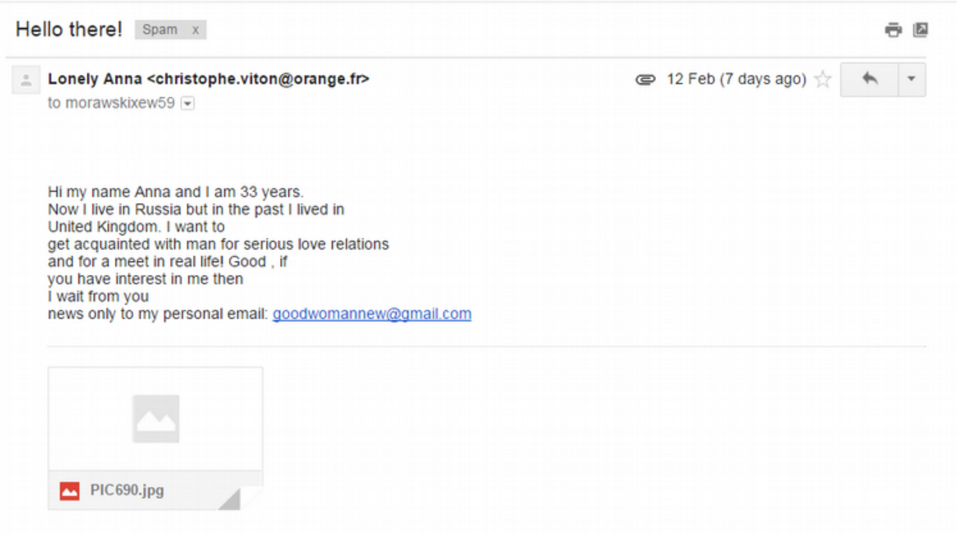
God bless you again my dear, I am Mrs Helen Smith, age 83 years old, I am the wife of late Mr. Bill Smith, I got your information's from my late husband diary we are both from United States Of America, my husband worked with Oil and Gas Company Chevron/Texaco in Africa for twenty years before he passed out.

When my late husband was alive he deposited the sum of $5.5million with Zenith Bank Nigeria Plc. in Africa Nigeria,Presently this money is still with the Bank, the bank management just send me an email to come over for the release of this money to me or i should rather issue somebody to receive the money on my behalf. Now I'm in a hospital in Netherlands where I have been undergoing treatment for cancer of the breast and Kidney including Pneumonia, the doctor told me i may not last up to 3 weeks because of my present situation.

Please i need your help to receive this money and use the money to help the less privilege once around you, I need your information so i can forward it to the bank to let the management know i have gotten you to receive my funds, I need your Full Name, Country/Address, occupation and Phone number. God Bless you once again as i hope to read from you soon.

Yours Beloved Sister,
Mrs Helen Smith

What a wonderfully kind offer!

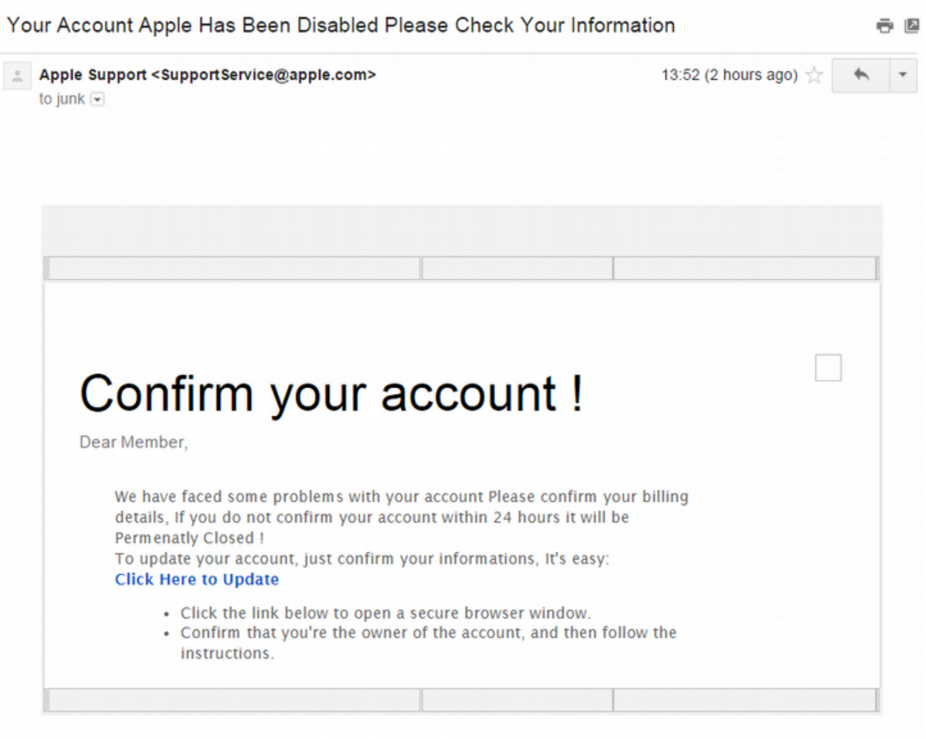


Hello there!

Lonely Anna <christophe.viton@orange.fr>
to morawskixew59

12 Feb (7 days ago)

Hi my name Anna and I am 33 years.
Now I live in Russia but in the past I lived in
United Kingdom. I want to
get acquainted with man for serious love relations
and for a meet in real life! Good , if
you have interest in me then
I wait from you
news only to my personal email: goodwomannew@gmail.com



Your Account Apple Has Been Disabled Please Check Your Information

Apple Support <SupportService@apple.com> 13:52 (2 hours ago)

to junk

Confirm your account !

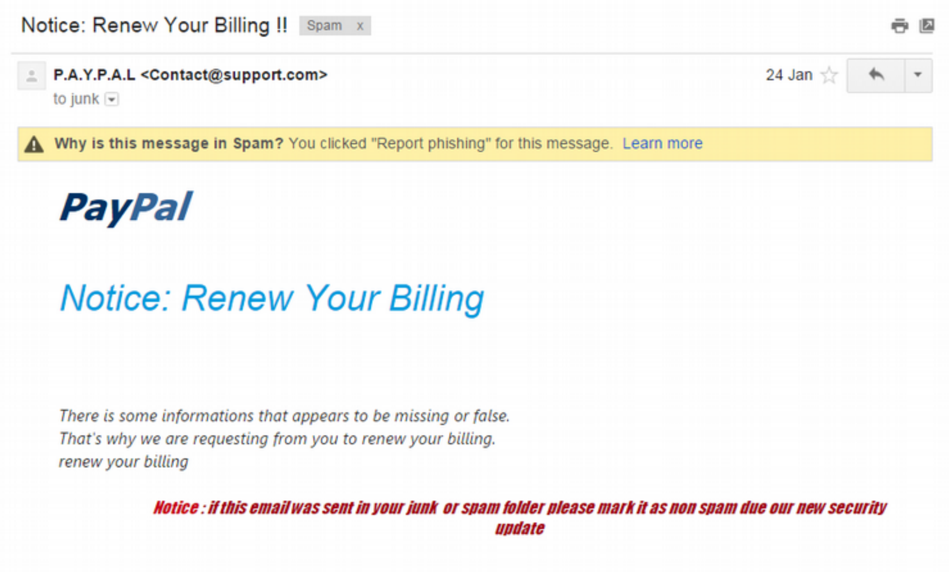
Dear Member,

We have faced some problems with your account Please confirm your billing details, If you do not confirm your account within 24 hours it will be Permenatly Closed !

To update your account, just confirm your informations, It's easy:

Click Here to Update

- Click the link below to open a secure browser window.
- Confirm that you're the owner of the account, and then follow the instructions.



Notice: Renew Your Billing !! Spam x

P.A.Y.P.A.L <Contact@support.com>
to junk

24 Jan

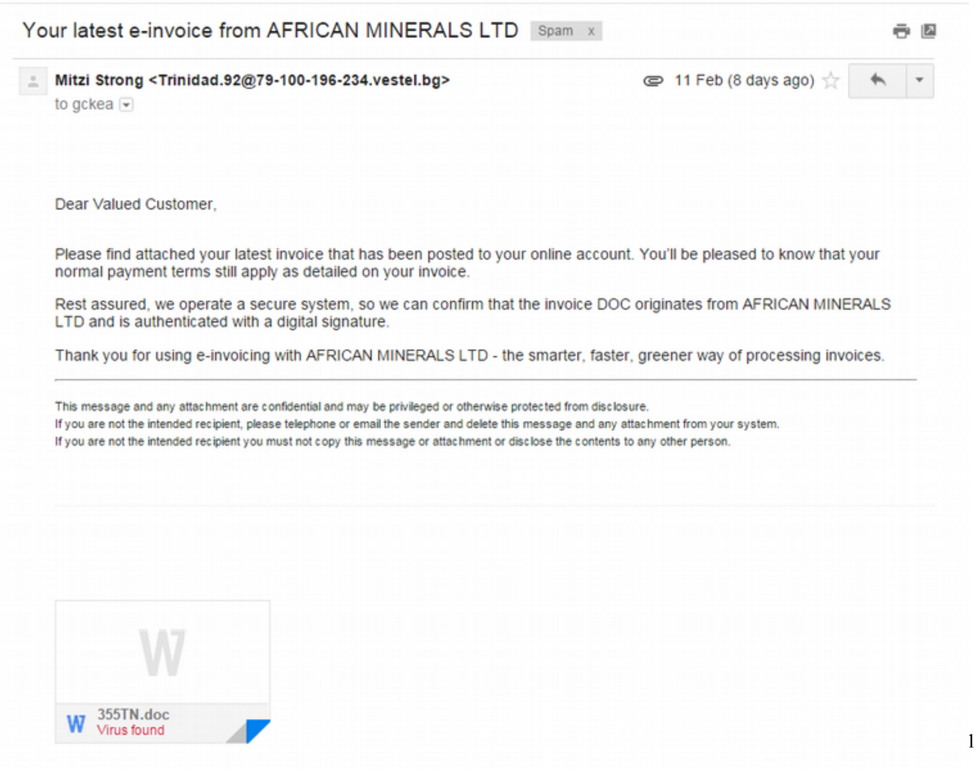
Why is this message in Spam? You clicked "Report phishing" for this message. Learn more

PayPal

Notice: Renew Your Billing

There is some informations that appears to be missing or false.
That's why we are requesting from you to renew your billing.
renew your billing

Notice : if this email was sent in your junk or spam folder please mark it as non spam due our new security update



Your latest e-invoice from AFRICAN MINERALS LTD

Mitzi Strong <Trinidad.92@79-100-196-234.vestel.bg>

to gckea

11 Feb (8 days ago)

Dear Valued Customer,

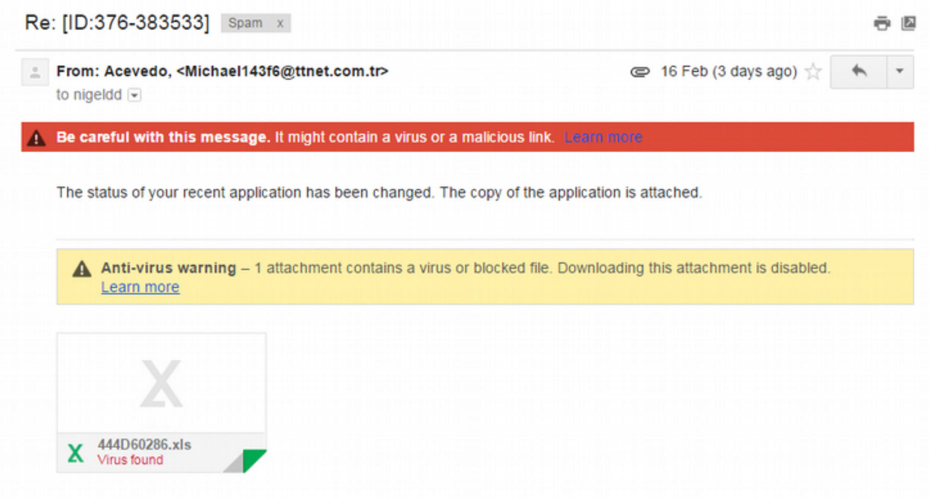
Please find attached your latest invoice that has been posted to your online account. You'll be pleased to know that your normal payment terms still apply as detailed on your invoice.

Rest assured, we operate a secure system, so we can confirm that the invoice DOC originates from AFRICAN MINERALS LTD and is authenticated with a digital signature.

Thank you for using e-invoicing with AFRICAN MINERALS LTD - the smarter, faster, greener way of processing invoices.

This message and any attachment are confidential and may be privileged or otherwise protected from disclosure.
If you are not the intended recipient, please telephone or email the sender and delete this message and any attachment from your system.
If you are not the intended recipient you must not copy this message or attachment or disclose the contents to any other person.

355TN.doc
Virus found



Re: [ID:376-383533]

From: Acevedo, <Michael143f6@ttnet.com.tr>

to nigeldd

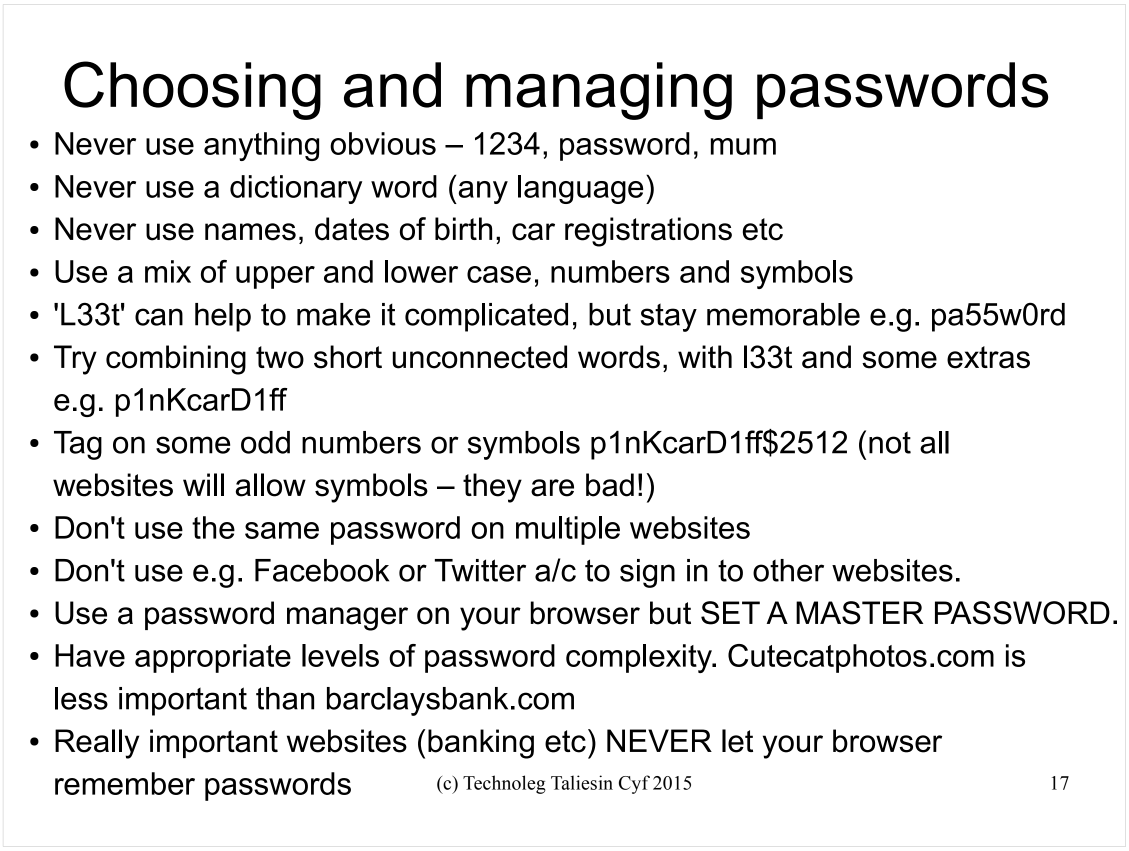
16 Feb (3 days ago)

Be careful with this message. It might contain a virus or a malicious link. Learn more

The status of your recent application has been changed. The copy of the application is attached.

Anti-virus warning – 1 attachment contains a virus or blocked file. Downloading this attachment is disabled. Learn more

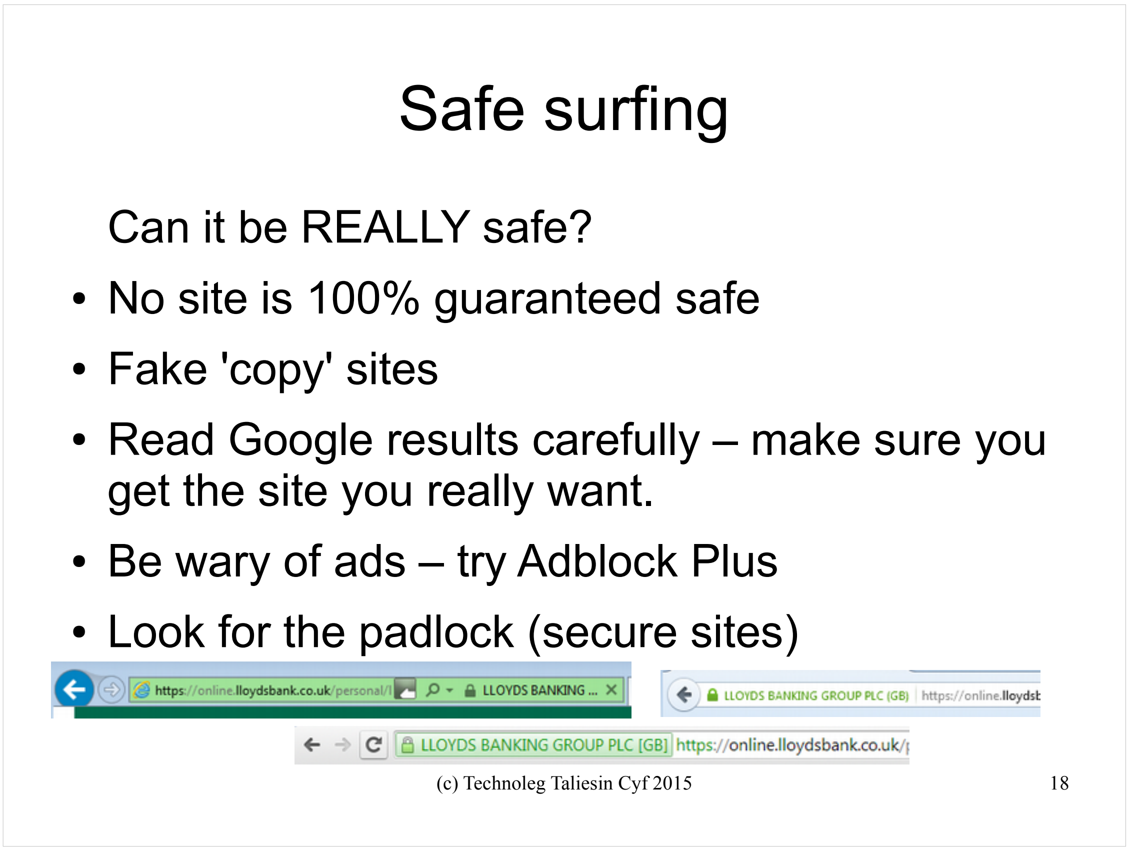
444D60286.xls
Virus found



Choosing and managing passwords

- Never use anything obvious – 1234, password, mum
- Never use a dictionary word (any language)
- Never use names, dates of birth, car registrations etc
- Use a mix of upper and lower case, numbers and symbols
- 'L33t' can help to make it complicated, but stay memorable e.g. pa55w0rd
- Try combining two short unconnected words, with l33t and some extras e.g. p1nKcarD1ff
- Tag on some odd numbers or symbols p1nKcarD1ff$2512 (not all websites will allow symbols – they are bad!)
- Don't use the same password on multiple websites
- Don't use e.g. Facebook or Twitter a/c to sign in to other websites.
- Use a password manager on your browser but SET A MASTER PASSWORD.
- Have appropriate levels of password complexity. Cutecatphotos.com is less important than barclaysbank.com
- Really important websites (banking etc) NEVER let your browser remember passwords

It's an art form!



Safe surfing

Can it be REALLY safe?

- No site is 100% guaranteed safe
- Fake 'copy' sites
- Read Google results carefully – make sure you get the site you really want.
- Be wary of ads – try Adblock Plus
- Look for the padlock (secure sites)

https://online.lloydsbank.co.uk/personal/l
LLOYDS BANKING ...
LLOYDS BANKING GROUP PLC (GB)
https://online.lloydsb
LLOYDS BANKING GROUP PLC [GB]
https://online.lloydsbank.co.uk/

The M&S website recently got infected – via an ad from another website

Sometimes an entire site can be copied perfectly, under a different name – but with added malware! e.g. johnlewis.com instead of johnlewis,co.uk

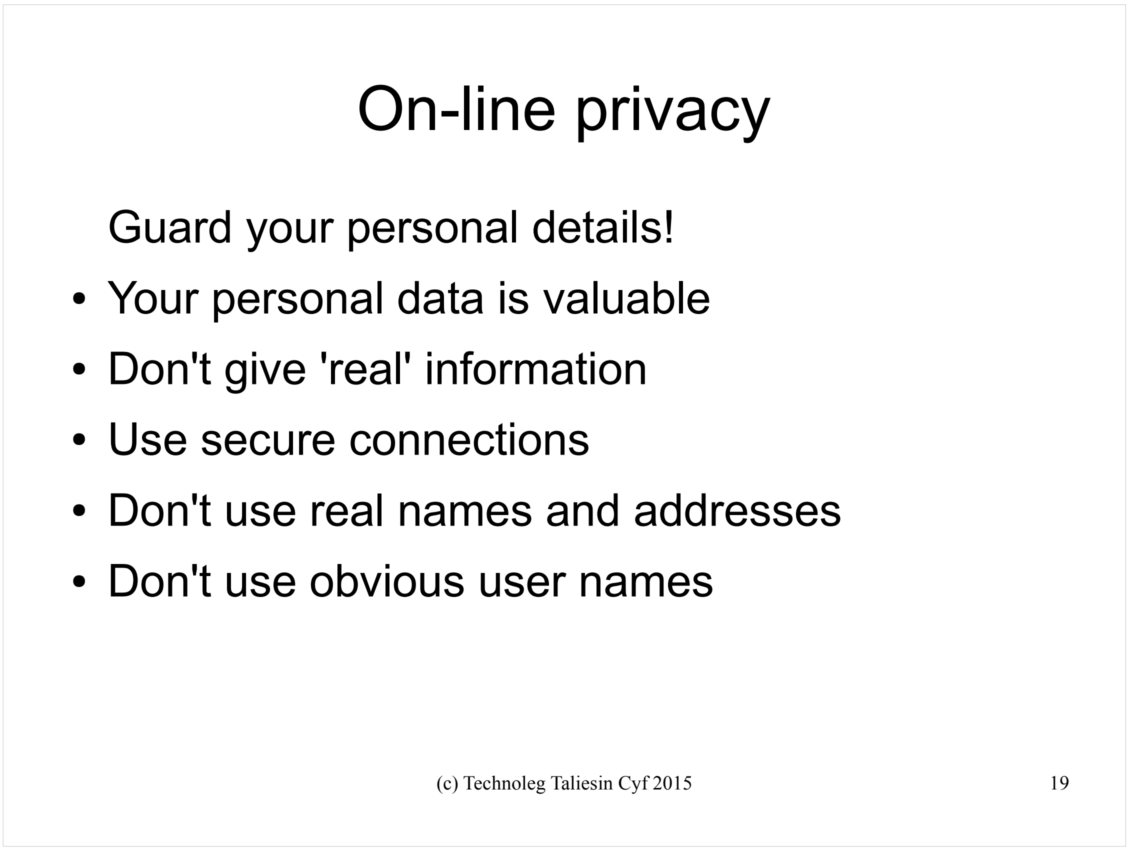
Ads (from other websites) can be infected/malicious – keep AV up to date! But still not guaranteed to be safe ('zero-day' exploits)

Worth installing Adblock Plus

Be particularly careful with banking, and anything else with personal information. Any good site will use HTTPS (secure connection) to encrypt all your data – look out for the green padlock (or similar)

Be wary of entering important information into insecure sites.

For banking sites, many use Rapport Trusteer for added security.



On-line privacy

Guard your personal details!

- Your personal data is valuable
- Don't give 'real' information
- Use secure connections
- Don't use real names and addresses
- Don't use obvious user names

Think of those 'security questions' they ask you.

Is your mother's maiden name or your date of birth public knowledge?

Try giving (memorable) false information – but obviously not to the tax man or bank! But why does John Lewis need your actual date of birth. Keep a record of your answers though.

User names and e-mail addresses – use something fairly meaningless if possible e.g. bluebiscuit@gmail.com rather than sallyjonestaliesin170397@hotmail.com

Be wary who you 'friend'.

Be wary about publishing photos online

Do you actually KNOW who welshmoggie27@hotmail.com is?

That's all folks!

- Copies of the slides, notes and links to the software mentioned are available at

  http://www.technoleg-taliesin.com

Professional website design for Wales

Creating wonderful websites since 2002

Technoleg Taliesin is a website design company based in North Ceredigion and so is ideally located to meet the IT needs of customers in Mid and West Wales, and further afield.

Trust no-one and nothing!

but have fun anyway...