Disclaimer

These documents have been prepared for my own use.
You are welcome to download and use them but I accept no liability for their content or anything arising from the use of the material they contain.

Staying Safe On Line

Andrew Knowles

The Ultimate Solution

- Don't buy a computer – if you already have one
- Don't turn it on – too late I turned it on
- Don't connect it to the internet

Risk Management

- There is no 100% secure solution but with a little knowledge you can use your computer and the internet with a minimum or risk
- Your risk level depends on what you use your computer for

What do you do

- Internet browsing (depending on sites visited)
- Video calling (Skype)
- Shopping
- Banking
- Store personal data/photos
- Email
- On-line auctions/payments
- Download music or software
- Allow remote access to your computer

Some Questions (1)

- When you start your computer, do you need to use a password to log in?
- When you leave your computer for a break, does it require you to enter a password be-fore you can start working again?
- Where do you keep your passwords for your computer and for logging on to websites and social media?
- Do you use a single password on more than one website?

Some Questions (2)

- Do you use antivirus software on your computer?
- Do you regularly update the software you use?
- Do you use a firewall on your router or on your computer to protect you from attackers?
- Do you have backups of your important data stored somewhere other than your computer (such as on another disk drive, computer or in the cloud)?

Some Questions (3)

- Have you ever been the victim of a computer-crime such as a virus or other malicious soft-ware or online fraud?

What are the risks

- Financial loss
- Theft of your identity
- Theft or destruction of your data
- Virus infection of your computer

How does this happen

- YOU provide confidential information to an attacker (Phishing E Mails, Phone Scams)
- Your confidential data held by organisations is accessed (Talk Talk Data breach)
- Your computer is infected with a virus or Malware

How does this happen

- Weak passwords
- Email account hacks
- Email scams
- Virus infections
- Out of date software

Jargon Buster

- ## Phishing

  the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.

- ## Malware

  software which is specifically designed to disrupt or damage a computer system.

- More details www.sophos.com/en-us/security-news-trends/security-trends/threatsaurus.aspx

Passwords

Passwords (1)

- DO NOT use the same password on more than one site or account.
- Change passwords on sensitive accounts regularly. (Bank accounts, credit cards, email accounts)
- Do not use easily guessable or dictionary words.
- Use long passwords (min. 15 characters mixing lower and upper case, numbers and symbols)

Passwords (2)

- No password is unbreakable given time and resources. Your password has to be sufficiently strong to make the time and effort spent breaking your password not worthwhile in relation to the returns it could provide.
- Do NOT save passwords on your computer or device.
- NEVER “Remember me” on any site
- Always set “auto logout” on all sites containing critical information.

Top 10 most commonly used

1	password
2	123456
3	12345678
4	1234
5	qwerty
6	12345
7	dragon
8	pussy
9	baseball
10	football

Lists of commonly used passwords can be found on the internet and it is very easy to write a program to write a program to try 1000's of passwords in a few seconds

What is a good password?

- Here is a reasonably strong password
- 5#GfPc7ke!QjX9FxB$
- Use a Password Manager
  (some examples but many others exist)

LastPass ****

dashlane

1Password

Another solution

- This solution is **NOT** recommended but it is better than using the same password on multiple accounts
- Using a phrase you can remember easily
  Jack and Jill went up the hill to fetch a pail of water
  JaJwuthtfapow
  J&Jwuth2fapow
- Add some extra characters to make it specific (eg Npower)
  J&Jwuthr6Nfapow!

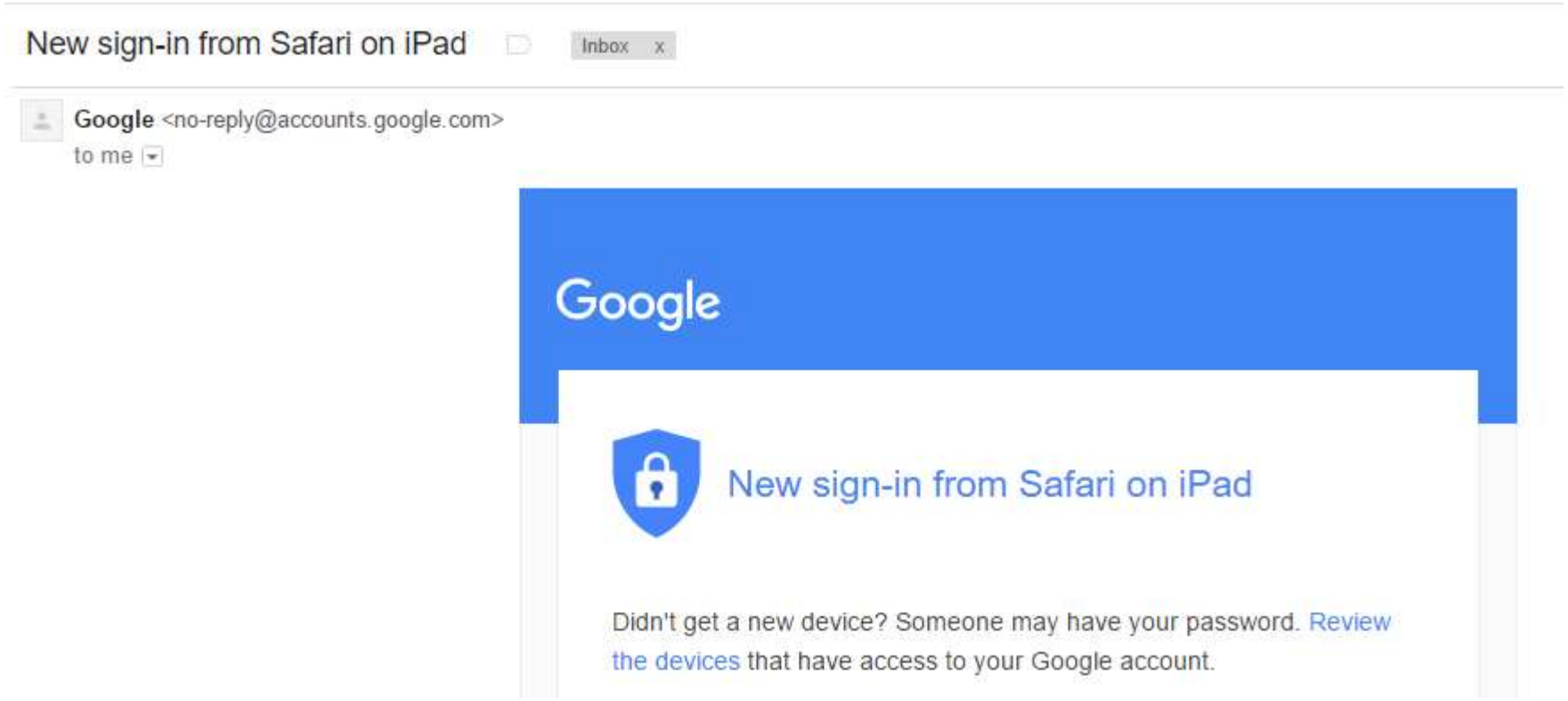
Two Factor Authentication

Two Factor Authentication

- Something you know – password
- Something you own – mobile phone

- 2FA can be enabled on many sensitive sites
  eg. Google, Cloud Storage, Password Manager

Trusted devices



Email account hacks

Email account hacks

- You will probably find that you can no longer connect to your email as the hacker will have changed your password
- The hacker can now pose as you (identity theft) using your email account
- The hacker can read your emails which may contain confidential information
- The hacker can steal or delete your address book

Email account hacks

- Protect your email account with a strong password and use 2 factor authentication
- Do NOT use public computers (libraries, cafe etc.) or public WiFi hotspots to log into your email account, internet banking etc.
- If you need to access your email or bank from a public location use your mobile 4G data connection

Email attachments

Email attachments

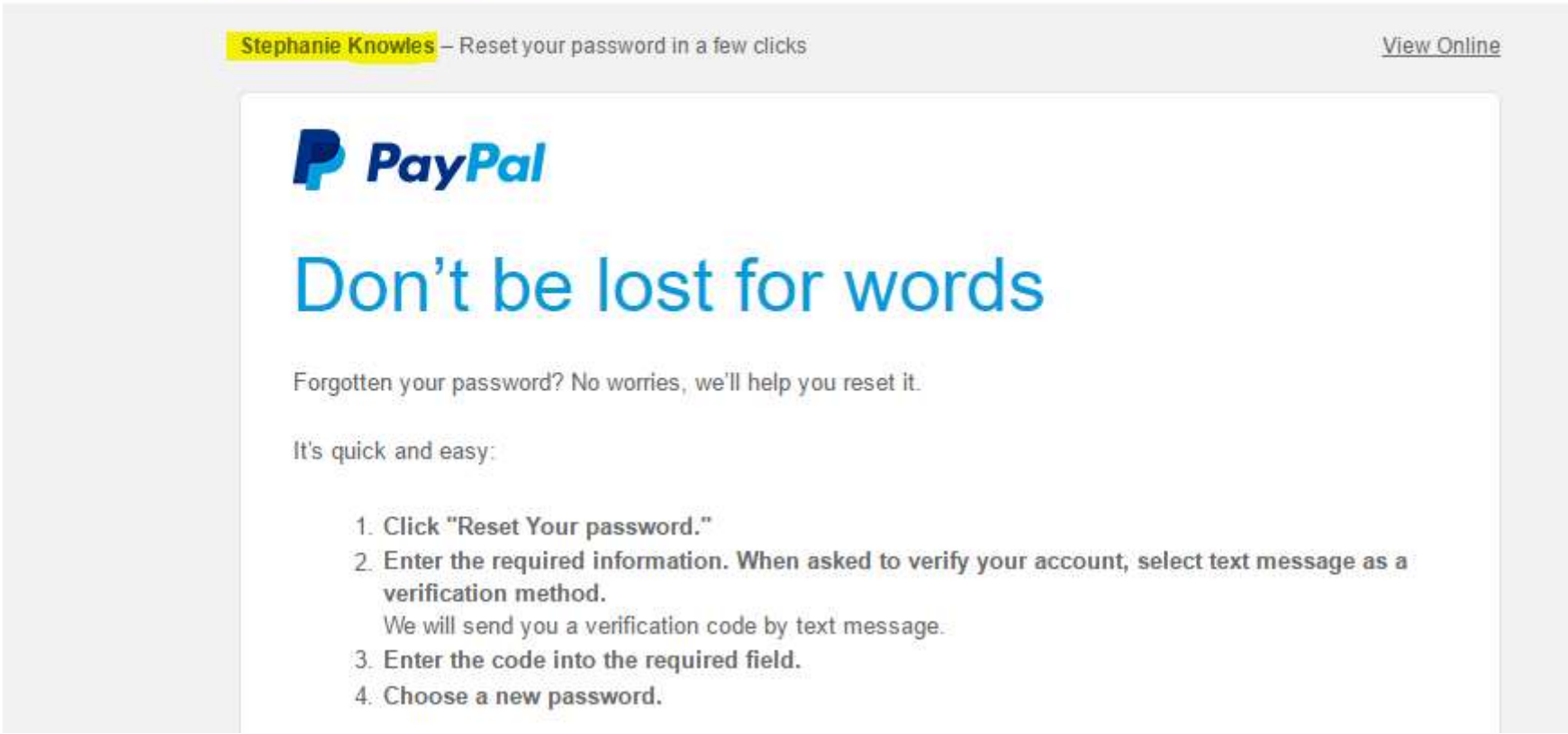
- Be suspicious of ALL attachments
- It is easy to disguise a virus file as a.pdf or .doc file

- Do not open any attachments from people you do not know
- THIS IS PROBABLY YOUR BIGGEST RISK OF GETTING A VIRUS

Email scams

PayPal Example (1)

From: "PayPal" <paypal@e.paypal.co.uk>
Subject: Forgotten your password? Reset it via text
Date: 16 March 2016 18:13:26 GMT
To: [redacted]@gmail.com
Reply-To: "PayPal" <noreply@e.paypal.co.uk>



Stephanie Knowles – Reset your password in a few clicks View Online

PayPal

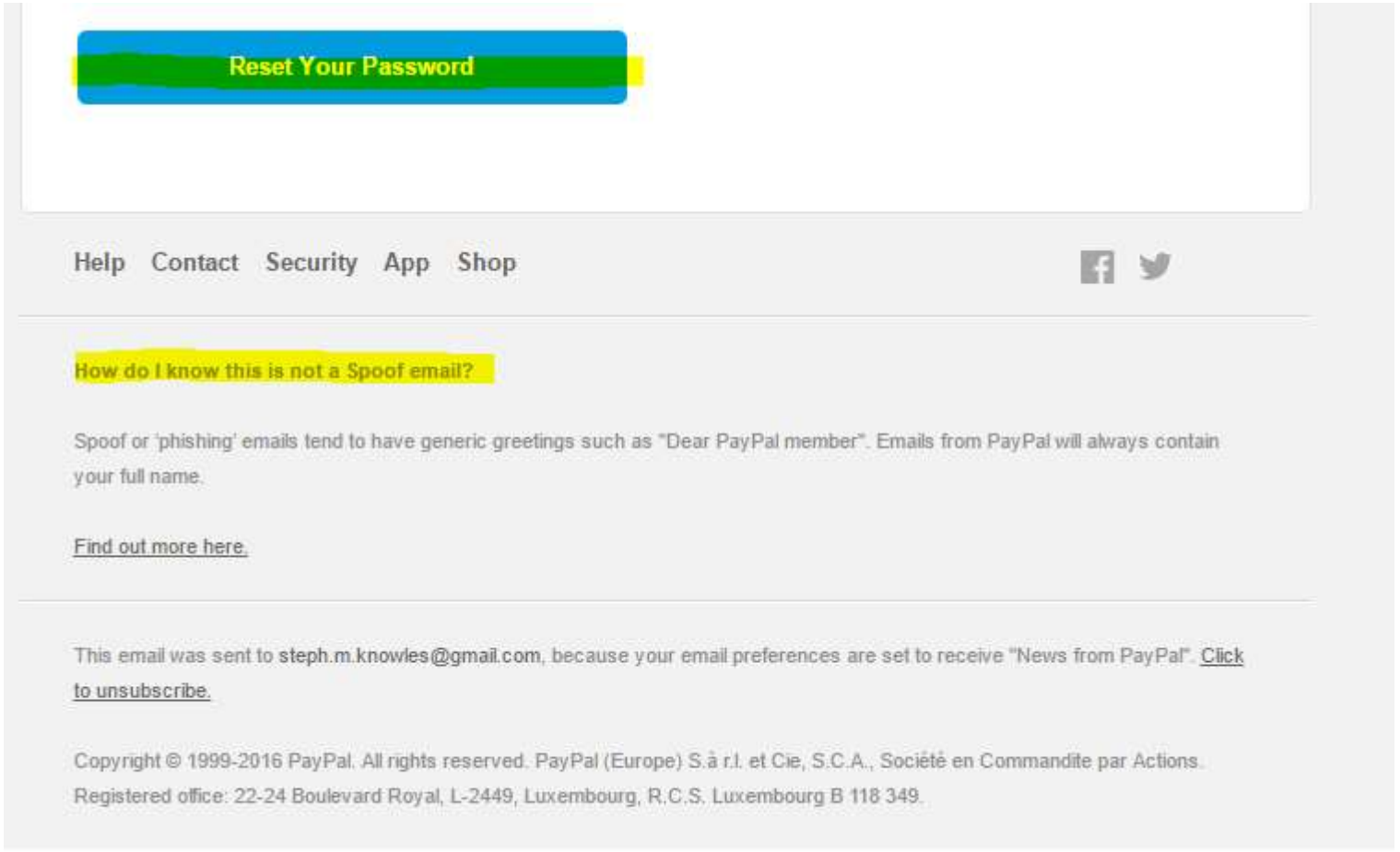
Don't be lost for words

Forgotten your password? No worries, we'll help you reset it.

It's quick and easy:

1. **Click "Reset Your password."**
2. **Enter the required information. When asked to verify your account, select text message as a verification method.**
   We will send you a verification code by text message.
3. **Enter the code into the required field.**
4. **Choose a new password.**

PayPal Example (2)



PayPal example evaluation

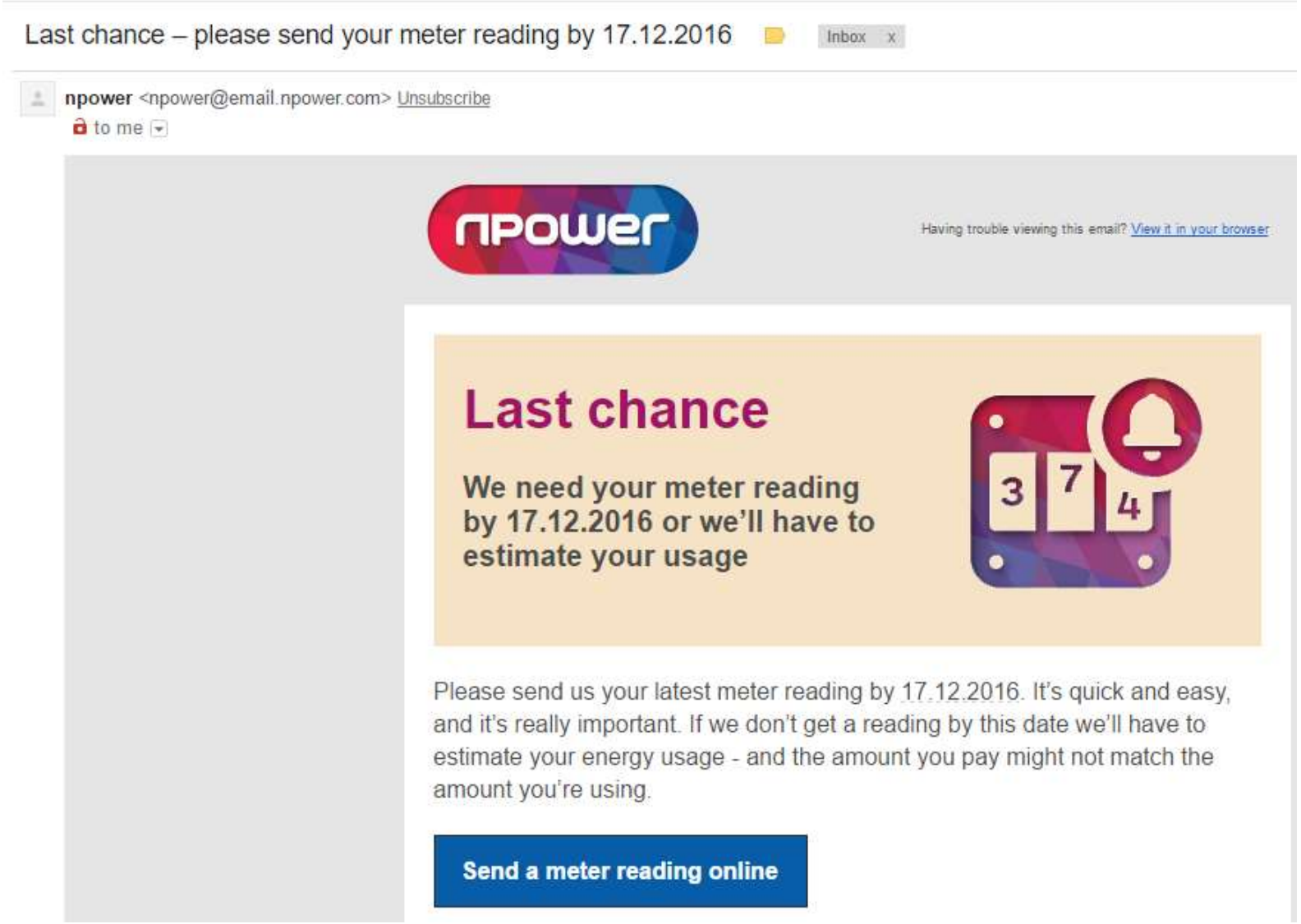
- Looks like a genuine PayPal email – no spelling mistakes, warnings about scam emails etc.
- Mail is from e.paypal.co.uk (no idea if this is a genuine Paypal site – Google “who is e.paypal.co.uk)
- Addressed to a specifically to you (positive point)
- The link directs you to https://email-edg.paypal.com/……(no idea if this is a genuine Paypal site – Google “who is email-edg.paypal.com)

PayPal example evaluation

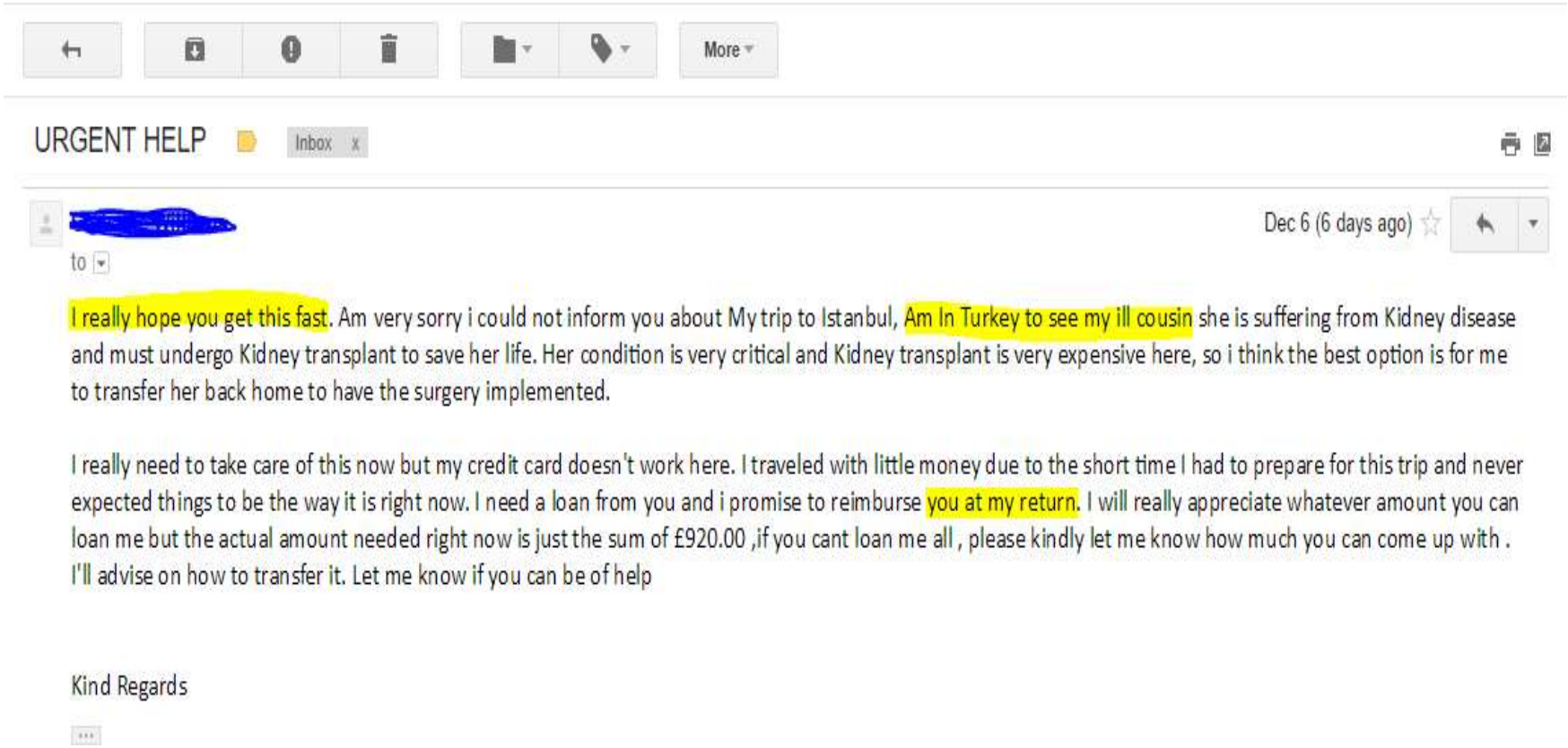
- From Google it appears that many people are suspicious of this address. On balance it is probably genuine and part of PayPal market-ing.

- BUT WHY TAKE THE RISK ! If you want to change your password go directly to the PayPal site at paypal.com and delete this email.

Email scams


Last chance – please send your meter reading by 17.12.2016
Inbox x
npower <npower@email.npower.com> Unsubscribe
to me
npower
Having trouble viewing this email? View it in your browser
Last chance
We need your meter reading by 17.12.2016 or we'll have to estimate your usage
3 7 4
Please send us your latest meter reading by 17.12.2016. It's quick and easy, and it's really important. If we don't get a reading by this date we'll have to estimate your energy usage - and the amount you pay might not match the amount you're using.
Send a meter reading online

Email scams



More

URGENT HELP Inbox x

[redacted]

Dec 6 (6 days ago)

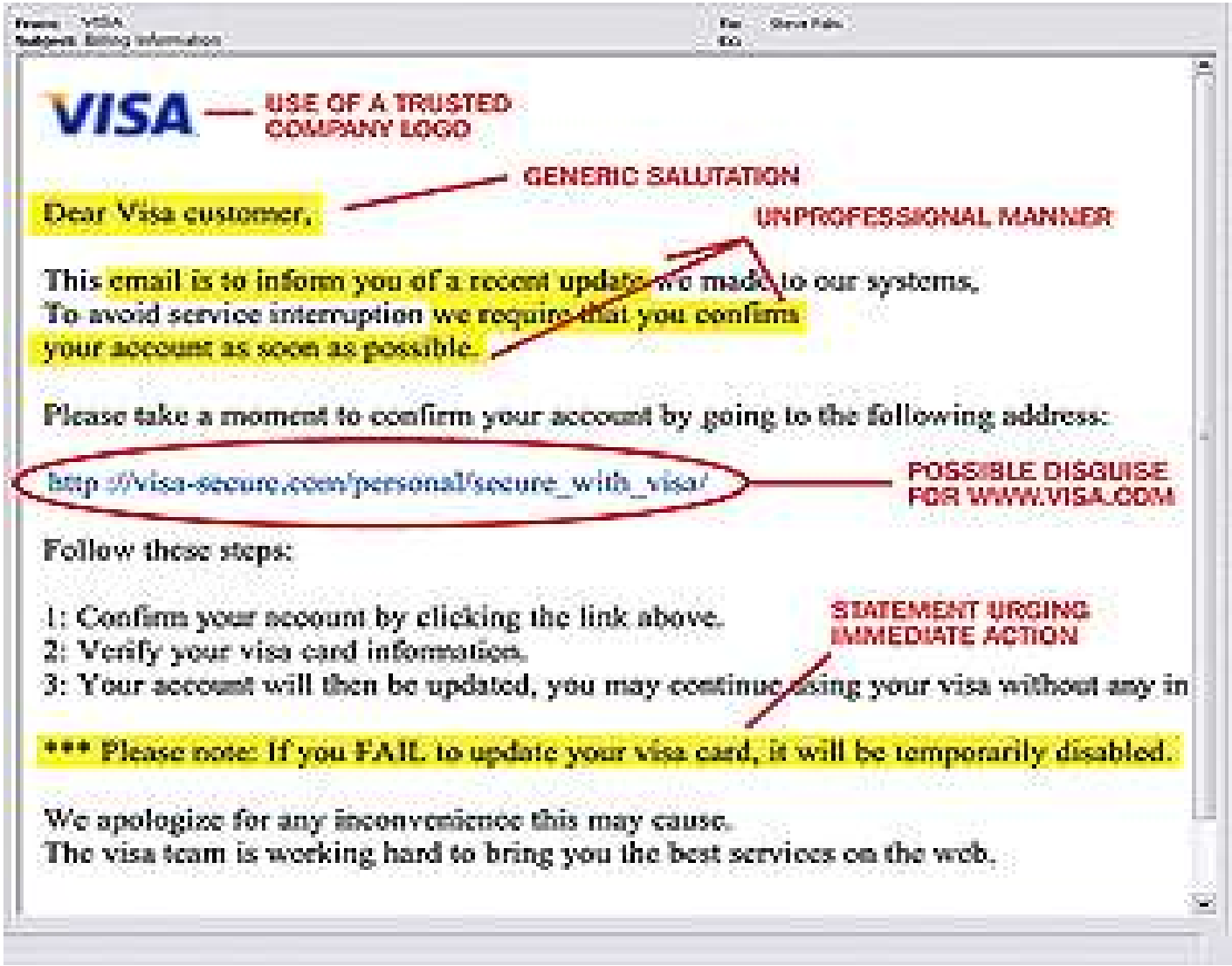
to

I really hope you get this fast. Am very sorry i could not inform you about My trip to Istanbul, Am In Turkey to see my ill cousin she is suffering from Kidney disease and must undergo Kidney transplant to save her life. Her condition is very critical and Kidney transplant is very expensive here, so i think the best option is for me to transfer her back home to have the surgery implemented.

I really need to take care of this now but my credit card doesn't work here. I traveled with little money due to the short time I had to prepare for this trip and never expected things to be the way it is right now. I need a loan from you and i promise to reimburse you at my return. I will really appreciate whatever amount you can loan me but the actual amount needed right now is just the sum of £920.00 ,if you cant loan me all , please kindly let me know how much you can come up with . I'll advise on how to transfer it. Let me know if you can be of help

Kind Regards

Email scams


VISA
USE OF A TRUSTED COMPANY LOGO
GENERIC SALUTATION
Dear Visa customer,
UNPROFESSIONAL MANNER
This email is to inform you of a recent update we made to our systems.
To avoid service interruption we require that you confirm
your account as soon as possible.
Please take a moment to confirm your account by going to the following address:
http://visa-secure.com/personal/secure_with_visa/
POSSIBLE DISGUISE FOR WWW.VISA.COM
Follow these steps:
1: Confirm your account by clicking the link above.
2: Verify your visa card information.
3: Your account will then be updated, you may continue using your visa without any in
STATEMENT URGING IMMEDIATE ACTION
*** Please note: If you FAIL to update your visa card, it will be temporarily disabled.
We apologize for any inconvenience this may cause.
The visa team is working hard to bring you the best services on the web.

Email scams


From: Westpac ID [mailto:mervilno@online.no]
Sent: Wednesday, 10 July 2013 12:54 p.m.
To:
Subject: Alert !
Not a Westpac email address
Scam email
Poor grammar and punctuation used in the email.
Dear Customer,
Your Defence Security has been suspended for protection of your account information and Online Transactions.
We hereby advise your for follow the Link below to Re-activate your WESTPAC Defence Security.
Activate Now
Don't click. Move your mouse over the link to see the URL, it usually points to a fake website. The URL will be displayed in the bottom left hand corner of your page.
With Westpac Defence you can be sure of a safe and securebanking environment.

Email scams

HSBC | The world's local bank

Dear HSBC customer,

Due to some issues we hold against your account(s), we temporarily suspended access to your online use. You may be getting this message because you recently signed on from a different location or computer. In order to avoid further actions taken by our security department, please identify yourself and continue using our service as normal:

https://hsbc.co.uk/1/2/HSBCINTEGRATION/CAM10;jsessionid=0tva9duIDV_URL=hsbc.MyHSBC_pib/

http://hsbc-online.wpew.info/1/2/HSBCINTEGRATION/CAM10;jsessionid=0000tva9NQkofu4NIM7pUel5Tvn11j5bfvduIDV_URL=hsbc.MyHSBC_pib/index.html

Thank you.

Email scams

- Does the email address you by name
- Is the spelling and grammar correct
- Does it suggest there is need for urgent action
- Does it ask you to click on a link within the email

- If in doubt contact the organisation involved using phone number or email obtained from ANOTHER source

WiFi security

How secure is your WiFi?

- How many people know your WiFi password?
- Often printed on a label on the back of the router
- Once connected to your WiFi network it is possible to do anything to your PC

How secure is your WiFi

- It is possible to improve security by changing passwords and making other changes to your router
- GET HELP unless you know what you are doing

Public WiFi

- Public WiFi IS NOT secure
- Keep your connection time as short as possible

- Avoid doing anything where you have to enter passwords or any other confidential information
- Use your phones 4G data connection if possible

Backup – What's that?

Backup – What's that?

- Hard drives are mechanical devices and DO fail (usually at the worst moment)
- Computers/hard drives can be stolen or lost
- Some viruses (ransom ware) can encrypt the information making your files unreadable (unless you pay)

Backup – What's that?

- If you value your data you need to BACK IT UP (make a copy)
- This needs to be kept in a different physical location from the computer
- External hard drives/USB keys/DVD's are better than nothing
- Use “The Cloud”

Backup – What's that?

- What is “The Cloud”
- It is “Someone else's computer”
- You have to trust that “Someone” with your data
  - Major cloud storage companies are unlikely to loose your data
  - How confidential is your data ? If your data is that confidential you should encrypt it before storing it.

Backup – What's that?

- A “Cloud” backup strategy
- You will need 2 Cloud accounts
- First account is synchronised with your computer
- Second account is not automatically synchronised
- Dropbox, One Drive(Microsoft), Google Drive

Backup – What's that?

- First account is automatically synchronised as you make changes on your computer
- Second account is MANUALLY SYNCHRONISED
- WHY ? - Ransom ware attacks
- If your computer is attacked by a ransom ware virus all files on your hard drive will be encrypted – including those automatically synchronised to your first account

Anti-virus

Anti-Virus (Windows)

- Windows 7 introduced “Microsoft Security Essentials” as standard. It is automatically activated and updated
- “Microsoft Security Essentials” was renamed as “Windows Defender” in Windows 10

- “Windows Defender” is considered as an acceptable solution in “low risk environments” but it is not the most sophisticated. It has low impact on performance and does not pester you with advertisements and offers.

- Many other programs exist (paying and free) Some of these will install other unwanted programs and/or browser extensions. Take care when installing

Anti-Virus (Windows)

- All Windows versions (since XP SP2) include a FIREWALL
- This is automatically activated unless someone turns it off. No need to touch this under most circumstances
- “SmartScreen Filter” helps you identify reported phishing and malware websites and also helps you make informed decisions about downloads

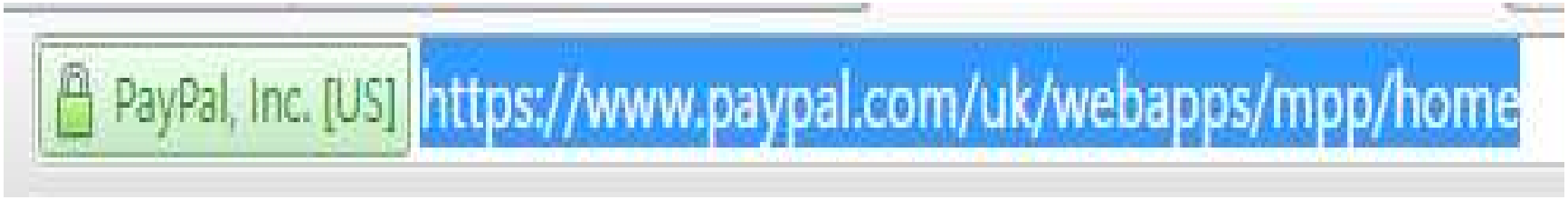
Anti-Virus (Windows)

- You may also want to run a “Malware Scanner”
- Best known is “Malware Bytes”
- Basic version is free but has to be run manually

Anti-Virus (Apple Mac)

- Apple have said that it is not necessary on Mac. Nothing built into the OS
- Now widely disputed and there are many products on the market (paid and free)
-
- Malware Bytes is also available for Mac

Browser Updates



- Latest versions of browsers show you the owner of the domain you are connecting to.

Summary

- Use strong and different passwords
- Always be suspicious – know the warning signs
- Keep your operating system up to date
- Keep your software up to date
- Install anti-virus software and keep it up to date
- Keep backup's of important data