Dacorum U3A

Computer Support Group

26th February 2021

Agenda

- General discussion on the use of zoom
- Open forum
- Continue online safety presentation
- Tea and Coffee break (about 3.00 pm?)
- Continue Presentation
- Review of meeting

Staying safe online

This presentation extends the one from 30th October 2020.

It makes use of further information put out by Which

It also looks at some email issues that may be of interest

Also the ‘life’ of SSD memory

Contents

I will cover the following:

- Online banking
- Passwords
- Data Breaches
- Paypal
- Phishing
- Scams
- ‘Spy’ Pixels
- SSD life

Online Banking

Which has an article which provides a ‘score’ of the security of their online bank access. I am not legally allowed to reproduce these scores.

However, I can describe the factors making up these scores.

Rather surprisingly, the article doesn’t analyse the security of mobile banking apps used by about 50% percent of users. It does imply that they are ‘better’ but then states that last year there was a 94% rise in fraud through the mobile apps.

Online Banking 2FA

Last time I went through Two factor Authentication (2FA).

In practice, the ’best’ way to do this is to have a separate device which takes a smart card so that a PIN can be checked and an authorisation code can be manually copied into the site.

An authorisation code telephoned to the user is also good. Although it is sometimes only for some of the actions. (The HMRC logon site uses this).

Slightly less good is to have a devices which can check a ‘PIN’ and generate the authorisation code.

Text ‘passwords’ are consistently marked down.

Online Banking Security Headers

Web Pages contain not only the HTML text but also ‘headers’. These are not normally visible to the user. Nor are they easy to describe!

New headers can be added. In particular new ‘security’ headers were added recently. Not all online banking sites have implemented these making them less secure than those that do.

Clickjacking Prevention – prevents a hacker from mirroring clicks into their own ‘frame’.

HTTP Strict Transport Security (HSTS) – ensures that ALL communication from this page use secure communications.

Online Banking Communications

TLS is the current version of SSL (secure socket layer – secure communication).

TLS 1.2 has been around since 2008 but is thought to have been ‘cracked’.

TLS 1.3 was defined in August 2018. This provides much improved security but has not been implemented by all online bank systems.

It is not clear whether all browsers actually support it.

Online Banking TLS 1.3 Browsers

Your browser version support TLS 1.3 if it is on one of these list

IE	Edge	Firefox	Chrome	Safari	Opera
			73		
		65	72		
		64	71	TP	
11	18	63	70	12	56 (4)
10	17	62	69	11.1	55 (4)
9	16	61	68	11	54 (4)
8	15	60	67	10.1	53 (4)

iOS Safari	Opera Mini	Android Browser	Blackberry Browser	Opera Mobile	Android Chrome
12	all	67	10	46	70
11.3-11.4		4.4.3-4.4.4	7	12.1	
11.0-11.2		4.4		12	
10.3		4.2-4.3		11.5	

Android Firefox	IE Mobile	Android UC Browser	Samsung Internet	QQ Browser	Baidu Browser
63	11	11.8	7.2	1.2	7.12
	10		6.2		
			5		
			4		

Online Banking Other

Some banks allow multiple concurrent sessions. This is seen as being a potential problem as it could allow a sessions on different devices to be cloned.

Where it is necessary to confirm logout is seen as being unnecessarily complex.

A previous login date and time is seen as good.

Some banks allow the user to leave a page and then come back again later.

Passwords

All passwords should be different. However, it is difficult to remember them all.

What are the alternatives:

- Record the password in an form that only you can decode.
  eg. F… might mean Fido or F..0 might be Fid0. It could be a combination of many of these.
  This would be difficult for a third party to decode.
- Use password recording software to save and generate a random password.
- Use your email app (eg. Thunderbird to remember you password).
- Use your browser app (eg. Firefox to remember your passwords.)
- Change your password every time you log on.

Password File

Using this approach to saving passwords:

- Difficult to record completely random passwords
- Difficult to safely record where letters should be replaced by numbers
- Not automatically copied to all devices
- Sometimes not easy to decode the meaning!

Password App

Using this approach to saving passwords:

- Usually possible to coordinate across devices
- May not work in all circumstances (eg library access PIN)
- Doesn’t work with selecting letters from a ‘word’
- Can usually create a completely random password
- May not be possible to backup and restore the data

Password in software

Using this approach to saving passwords:

- Not usually possible to coordinate across devices
- May not work in all circumstances (eg library access PIN)
- Doesn’t work with selecting letters from a ‘word’
- Thunderbird storing email passwords is automatic but can be turned off
- Thunderbird can display the email passwords
- Firefox you can select to save the password for a particular form (site) or not

Data Breaches

This section is not about your computer being hacked but about big companies leaking data so that ‘your’ personal data may be compromised.

The list below shows some of the companies that have had the personal data they hold hacked or otherwise ‘lost’ their recorded data.

In most cases the data is available for sale on the dark web. Or in some cases blackmail is the outcome.

Data Breaches 2

Year	Company	Breach
2005	Designer Shoe Warehouse	First known data breach (US)
2007	HMRC	2 CDs with more than 25 million records ‘lost’
2008	Heartland Payment Systems	More than 100million card records stolen (US)
2011	Sony	20,000 credit card and bank details
2012	Linkedin	165million accounts stolen
2013	Adobe	15million accounts exposed in hack
2014	ebay	145million personal data and passwords
2014-6	Yahoo	3billion users impacted
2015	Ashley Madison	60gb stolen from extramarital affairs website
2016	MySpace	Data from 360 million users on sale
2017	Equifax	Data from 147million Americans and 15million UK citizens stolen from credit scoring company
2018	Various eg Marriott	1.8billion records in data breaches
2019	Collection #1	Provides database 773million emails and 21million passwords
2020	Psychotherapy..Finland	Patients report blackmail attempts

Data Breaches 3

It is probable that you should carefully consider whether you let third parties have any of your important data. This is especially true of card/account information but includes email ids and dates of birth.

Paypal

At the last meeting people suggested that using Paypal to make payment is better than using a credit card. Here are a few instances from Which where the use of Paypal was far worse:

Of course it can be quite expensive for the hacker to hack into systems. Where only a relative small amount of data is available a deliberate breach is less likely.

Below are couple of examples where it has gone wrong.

Paypal 2

Apparently, Paypal usually accepts a ‘tracking number’ as showing a valid delivery. To get round this, fraudsters will send a low value product, to get such a number.

Eg. a cheap manicure set was sent instead of a £35 decoration set for a wedding. Paypal refused a refund.

Paypal 3

Paypal ‘may’ refund if you ‘pay’ another account if you use the ‘goods and services option. It will refuse a refund if you select ‘friends and family’.

Paypal claim to cover only authorised transactions. When the host disappeared following £800 for an Italian holiday home rental, Paypal refused a refund as it was authorised. The bank was unable to help as legally the transaction was with Paypal not the home owner.

Phishing

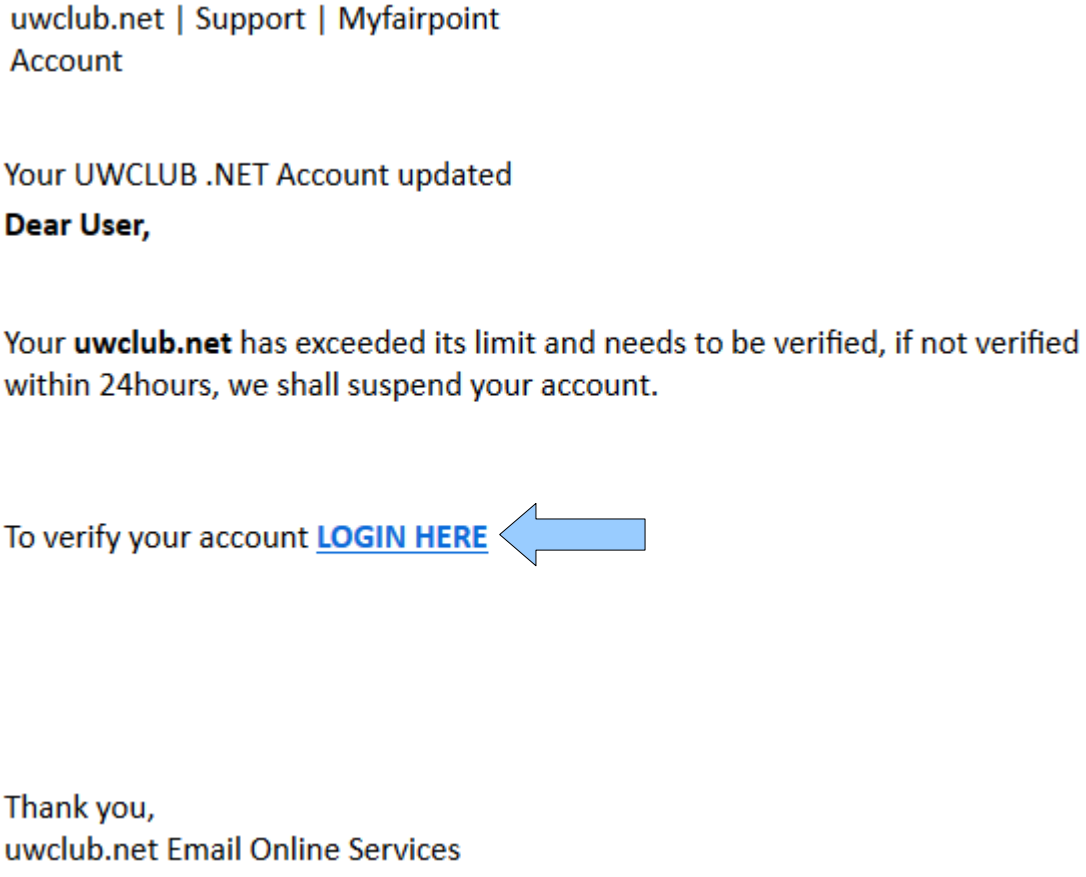
Phishing is an attempt to get login and/or other personal information by sending an apparently genuine email with a link in it.

Over the last week or 2, I have received many emails similar to that on the right.

One of the simple ways to see whether this is genuine is to see where the 'LOGIN HERE' link arrowed takes you. On thunderbird this can be by hovering the mouse over it or by right clicking on it.

This resolves as: '*uwchomcare.weebly.com/*'

This is obviously NOT uwclub.net



uwclub.net | Support | Myfairpoint Account

Your UWCLUB .NET Account updated

Dear User,

Your **uwclub.net** has exceeded its limit and needs to be verified, if not verified within 24hours, we shall suspend your account.

To verify your account **LOGIN HERE**

Thank you,
uwclub.net Email Online Services

Phishing 2

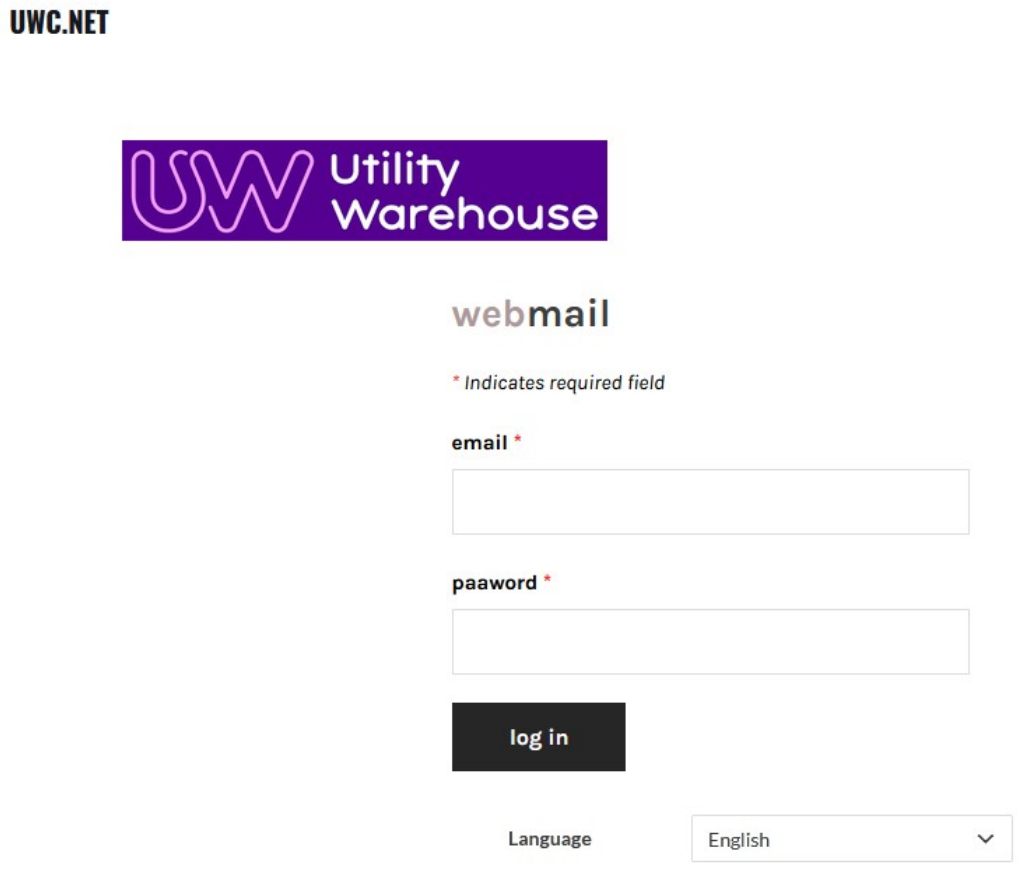
You should NOT click on the link as it could do untold harm (including confirming that the email address is genuine – see Spy Pixels below)

However, I know that in this case I can do it safely.

The resulting webpage is shown on the right.

Again I might be able to hover or right click the link. However, not in this case! It actually resolves as: '*www.weebly.com/weebly/apps/formSubmit.php*'

This would then record the userid and password and allow emails to be sent.



Phishing 3

Coincidently, this week, I received an email from my ISP with similar suggestions:

Look out for:

Email 'from' addresses
We'll never send you emails about your account being closed, updated or modified in any way from a @uwclub.net accoun
@hello.uw.co.uk

Website addresses
Our UW websites will be hosted at domains ending with uw.co.uk, with the exception of webmail.uwclub.net. When lookin

For example, the following websites are **not** official UW websites – they're hosted on godaddysites.com and weebly.com, n

Illustration of two fake UW websites with godaddy and weebly URLs

Never share details about your account with these sites. If you have already shared details, please change your passwor

Email content
Phishing emails tend to be demanding, and often add a sense of urgency by making it seem like something bad will happen

Phishing 4

What to do about it?

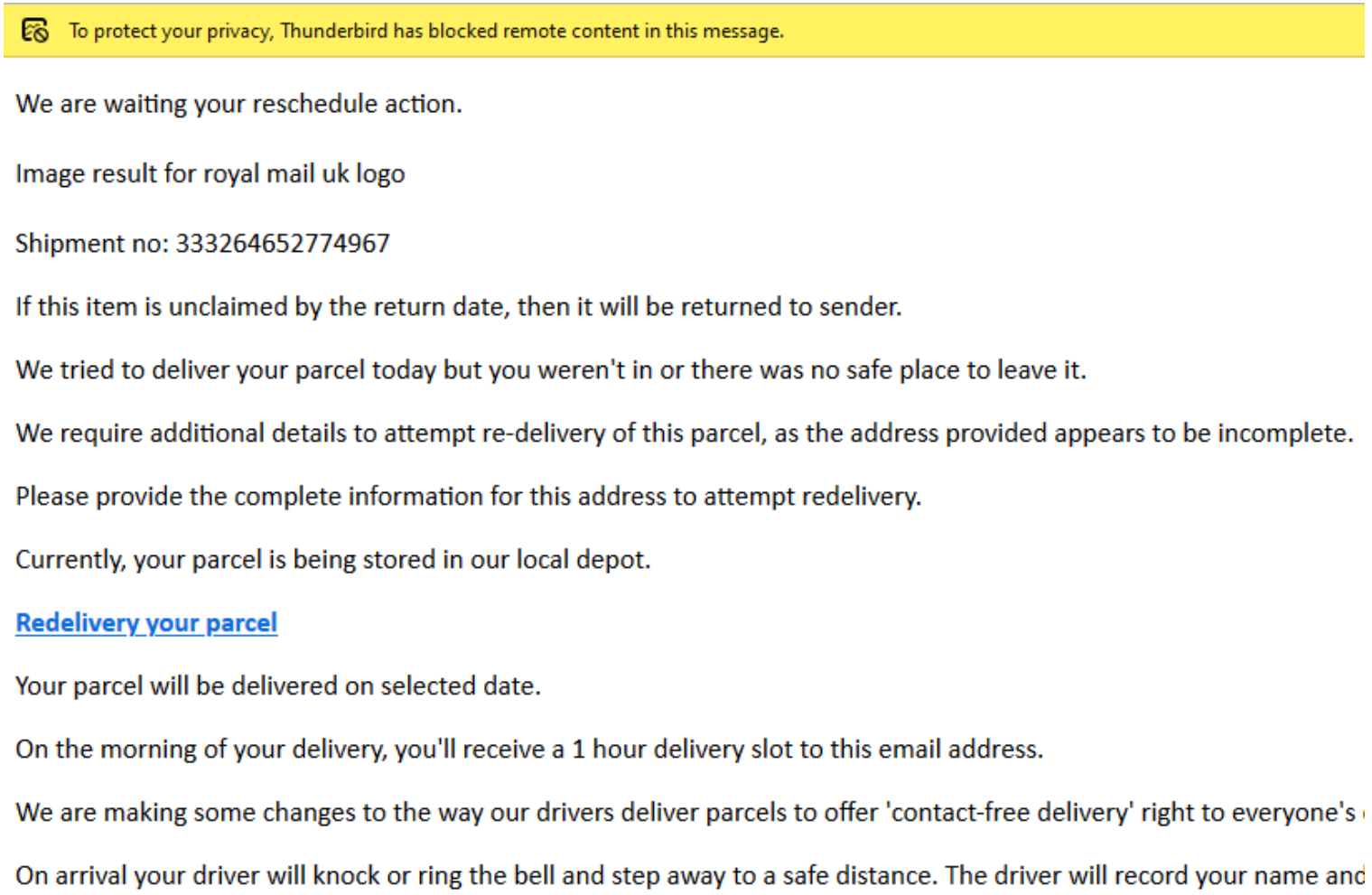
You can forward the email to one of:

- report@phishing.gov.uk
- phishing@hmrc.gov.uk

Most other banks and isps have their own fraud/phishing email addresses

Scam email

Here is an example of a scam email:



To protect your privacy, Thunderbird has blocked remote content in this message.

We are waiting your reschedule action.

Image result for royal mail uk logo

Shipment no: 333264652774967

If this item is unclaimed by the return date, then it will be returned to sender.

We tried to deliver your parcel today but you weren't in or there was no safe place to leave it.

We require additional details to attempt re-delivery of this parcel, as the address provided appears to be incomplete.

Please provide the complete information for this address to attempt redelivery.

Currently, your parcel is being stored in our local depot.

Redelivery your parcel

Your parcel will be delivered on selected date.

On the morning of your delivery, you'll receive a 1 hour delivery slot to this email address.

We are making some changes to the way our drivers deliver parcels to offer 'contact-free delivery' right to everyone's

On arrival your driver will knock or ring the bell and step away to a safe distance. The driver will record your name and

Scam email 2

How does this work?

If you click on the link, it will take to a website which will tell you about the ‘delivery’ and ask you amongst other things to pay a small amount for the extra delivery. This payment can be made by a card.

That is the last you will hear.

They can then claim the small fee from the card company. More importantly, they have ALL the card details to make more ‘payments’.

What can you do? - Immediately cancel the card and keep a look out for and charge back any subsequent transactions made on it.

The card and possibly any related ones will be will be cancelled and replaced. For this reason, it is probably a good idea to have another, unrelated one.

Scam email 2

That was fairly easy to spot, the English leaves something to be desired '*Redelivery your parcel*'! But the clincher in the url that goes with that - '*https://adtgroupholdings.com/vendor/swiper/css/sweiper/e0c8b6e2a0c294.html*'. It is unlikely that this has anything to do with parcel delivery (in Thunderbird, hover or right click over the request).

‘Spy’ Pixels

The BBC sent out an item entitled:

'Spy pixels in emails have become endemic'

The use of "invisible" tracking tech in emails is now "endemic", according to a messaging service that analysed its traffic at the BBC's request.

Hey's review indicated that two-thirds of emails sent to its users' personal accounts contained a "spy pixel", even after excluding for spam.

Its makers said that many of the largest brands used email pixels, with the exception of the "big tech" firms.

‘Spy’ Pixels 2

What are ‘spy’ or ‘tracking’ pixels. They form part of the ‘text’ of an email. They mean that a request will be sent to the internet when the email is opened.

Tracking pixels are typically a .GIF or .PNG file that is a small as 1x1 pixels, which is inserted into the header, footer or body of an email.

Since they often show the colour of the content below, they can be impossible to spot with the naked eye even if you know where to look.

Recipients do not need to click on a link or do anything to activate them beyond open an email they are embedded in.

British Airways, TalkTalk, Vodafone, Sainsbury's, Tesco, HSBC, Marks & Spencer, Asos and Unilever are among UK brands Hey detected to be using them.

‘Spy’ Pixels 3

What can they do?

Emails pixels can be used to log:

if and when an email is opened

how many times it is opened

what device or devices are involved

the user's rough physical location, deduced from their internet protocol (IP) address - in some cases making it possible to see the street the recipient is on

This information can then be used to determine the impact of a specific email campaign, as well as to feed into more detailed customer profiles.

‘Spy’ Pixels 4 Privacy

Use of tracking pixels is governed in the UK and other parts of Europe by 2003's Privacy and Electronic Communications Regulations (Pecr) and 2016's General Data Protection Regulation (GDPR).

They require organisations to inform recipients of the pixels, and in most cases to obtain consent.

One privacy consultant said the Court of Justice of the European Union (CJEU) had previously ruled that such consent must be "unambiguous" and "a clear affirmative act".

"Solely placing something in a privacy notice is not consent, and it is hardly transparent," said Pat Walshe from Privacy Matters.

"The fact that tracking will take place and what that involves should be put in the user's face and involve them opting in.

"The law is clear enough, what we need is regulatory enforcement. Just because this practice is widespread doesn't mean it's correct and acceptable."

‘Spy’ Pixels 5 Example

Apologies for the complexity

Here is an email (sorry abut the size)

To protect your privacy, Thunderbird has blocked remote content in this message. Options

Message from the Chair

Dare I say a ‘Happy’ New Year? Perhaps it would be kinder and more relevant to say I wish you a ‘Better’ New Year, although at the moment that seems to be a thought too far! But with a flying wind and a full vaccination programme we will get through this together.

However, you may not have known that your committee are still meeting as usual, and with some additional meetings, thinking and planning ahead with a wish that before too long we shall all be able to meet again and plans are being made to be ready to re-start our U3A as soon as it is safe to do so. Your patience is appreciated.

Life is very different for us all and those of us who have been brave enough to face Zoom meetings have been able to see friends and to participate in some of our usual activities. If you haven’t been encouraged enough to try yet do please try. WhatsApp is keeping people in touch, and the telephone is invaluable.

You have heard, I know, that I have a now 98 year old mother, whose claim to fame is that she has me under her thumb, and about whom I am going to write a book. She had her birthday party with all the family on 9th January via Zoom and was incredibly pleased that she saw grandchildren and great grandchildren, all having an afternoon tea to celebrate. She hasn’t, I suspect like some of you, been out of the confines of her house and garden for what is now a year.

The committee is planning a zoom co-ordinator chat meeting in the not-too-distant future, to outline our plans for a staggered restart of our U3a. So if you are a coordinator, I hope you will be able to join in.

Keep safe everyone,

Tina

This email was sent by Beacon on behalf of secretary@u3adacorum.org

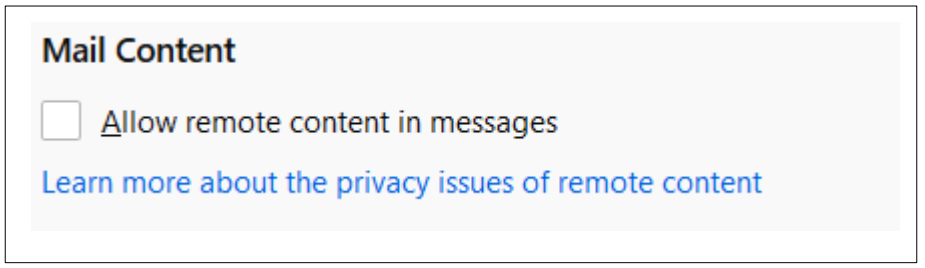
‘Spy’ Pixels 5 Example 2

Here is (part of what is sent):
... headers
Message from the Chair
Dare I say a =E2=80=98Happy=E2=80=99 New Year? Perhaps it would be kinder a=
nd more relevant to say I wish you a =E2=80=98Better=E2=80=99 New Year, alt=
hough at the moment that seems to be a thought too far! But with a flying w=
ind and a full vaccination programme we will get through this together.
… rest of message + more header information + repeat as html
<p class=3D"western"><span style=3D"font-family: Liberation Sans, sans-seri=
f;"><span style=3D"font-size: x-large;">Message from the Chair</span=
></p>
<p class=3D"western"><span style=3D"font-family: Liberation Sans, sans-seri=
f;"><span style=3D"font-size: medium;">Dare I say a ‘Happy’ New=
 Year? Perhaps it would be kinder and more relevant to say I wish you a
… most of rest of message + final line
<p class=3D"western"><span style=3D"font-family: Liberation Sans, sans-seri=
f;"><span style=3D"font-size: medium;">Tina</p><hr></br>This =
email was sent by Beacon on behalf of secretary@u3adacorum.org<img src=3D"h=
ttps://u2125344.ct.sendgrid.net/wf/open?upn=3DiuWMrNMHug
… more image information, identifying which message it is and size
border=3D"0" style=3D"height:1px !important;width:1px !important;border-wid=
…
/>

‘Spy’ Pixels 6 Thunderbird

Thunderbird has an option to prevent remote content being activated. By default this option in ‘on’. It is possible that other email clients have similar facilities.

To access this use ‘Options’ – Privacy and Security.



Spy Pixels 7

We will progress whether Spy Pixels can legitimately be included in Beacon ‘Group’ emails.

SSD Life

Many computers now have Solid State Drives (SSDs) rather than Hard Disk Drives (HDD).

SSDs consume about 50% of the power so are ‘better’ for laptops. They also provide much faster (random) access times so usually start the operating system much faster.

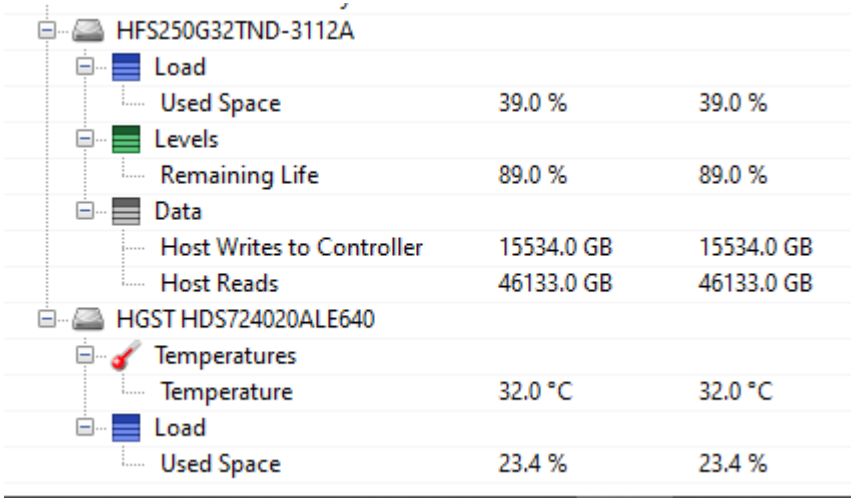
However, the number of ‘writes’ to each ‘cell’ is limited. So that the life of the SSD is limited, especially where it is used where there are a large number of writes (eg the ‘paging file’)

SSD Life 2

Here is the section of the OpenHardwareMonitor display for my desktop.

The top part relates to the SSD which holds the operating system.

Although this currently is only 39% used, 21% of the ‘life’ has been used in about 5 years. This represents writing 15.5 terabytes of data.



SSD Life 3

Reliability – SSD limited – HDD possible mechanical problems – unclear which is ‘better’

Longevity – SSD may lose data after 1-2 years (note applies to Pen drives) – HDDs limited by mechanical seizing

Random Access – SSD typically .1ms – HDD my easily be 12ms

SSD & Operating Systems

SSDs are usually direct replacements for HDDs so will work on most operating systems.

However, one of the important features of an SSD is TRIM which significantly improves performance. Not all operating systems automatically implement this.

LINUX doesn't implement this as standard

MacOS only supports it for Apple SSDs. Other types require extra facilities

Windows

Vista doesn't really support SSDs
7 has limited support
8.1 & 10 have support for SSDs with Trim for SATA connections

See Wikipedia

Summary

As I have said before:

Don’t Panic

Just Be Careful