

A brief guide to Passwords and Internet Security Part 2

Secure documents

Mendlesham Computer Club

By Giles Godart-Brown

Securing documents you have created

Both OpenOffice and Microsoft Office allow you to save a document or spreadsheet with a password so it can only be opened by someone who has the password (the key).

This is useful if you want to send a confidential document via email.

If you do this then you should send the password via a different route. I usually text passwords as this is a very secure mechanism.

Identity Theft

Mendlesham Computer Club

By Giles Godart-Brown

Identity Theft

Mendlesham Computer Club

By Giles Godart-Brown

What is Identity Theft?

Identity theft happens when someone uses your personal information without permission. This may include:

- Name and address
- Bank or credit card details
- National Insurance number
- NHS number

Criminals may:

- Take money from your accounts
- Open loans or credit cards
- Claim benefits or refunds in your name
- Create companies using your address

Warning Signs of Identity Theft

- Bank transactions you don't recognise
- Letters about debts or loans you never took out
- Missing post or unexpected mail
- Being refused credit for no clear reason
- Calls or emails asking for personal details

If something doesn't feel right, check it.

Step 1 – Don't Panic, Act Quickly

If you think your identity has been stolen:

- Stay calm
- Write down what has happened
- Keep letters, emails, and bank statements
- The sooner you act, the easier it is to fix



Step 2 – Contact Your Bank Immediately

- Call your bank using the number on your card or statement
- Tell them you suspect fraud
- Ask them to:
 - Stop suspicious payments
 - Freeze or close affected accounts
 - Issue new cards or passwords

Banks in the UK are required to help protect you.

Step 3 – Report It to Action Fraud

Action Fraud is the UK's national fraud reporting service.

- Report online or by phone
- They will give you a 'crime reference number'
- This helps banks, insurers, and police investigations

If you are in immediate danger, call 999

Step 4 – Protect Your Credit Record

- Contact one of the UK credit reference agencies:
 - Experian
 - Equifax
 - TransUnion
- Ask for a ‘fraud alert’ (also called a protective registration)
- Check your credit report for accounts you don’t recognise
- You can also register with ****CIFAS**** for extra protection.

Step 5 – Check Your Credit Report

- Look carefully for:
 - Loans or credit cards you didn't apply for
 - Incorrect addresses or personal details
- Report anything suspicious straight away.

Step 6 – Contact Other Organisations (If Needed)

- Depending on what was stolen:
 - HMRC– if tax or National Insurance details are involved
 - NHS – if your NHS number was misused
 - DWP – if benefits are affected
- They can place extra checks on your records.

Watch Out for Follow-Up Scams

- Criminals may pretend to:
 - Be from your bank
 - Offer to “recover” stolen money
 - Ask for fees or personal information
- Remember:
 - Banks and government departments will never ask for passwords
 - Hang up and call back using a trusted number

How to Protect Yourself in the Future

- Shred documents with personal information
- Never share PINs or passwords
- Be cautious with phone calls and emails
- Use strong, unique passwords
- Check bank statements regularly
- Ask a trusted friend or family member for help if needed.
- Register on Land Registry for property alerts

You Are Not to Blame

- Identity theft is common
- Anyone can be targeted
- Help is available
- Acting quickly makes a big difference

Useful UK Resources

- Action Fraud (<https://www.nafn.gov.uk/report/action-fraud/>) – report fraud
- Your bank or building society
- CIFAS (<https://www.cifas.org.uk/>) – identity protection
- Credit reference agencies
- Local council or community support services
- Property alert on Land Registry property.alert.landregistry.gov.uk

Security hints and tips Summary

Additional security mechanisms

- Most financial sites and some shopping sites now use 2 factor authentication, these need a smart phone and a connection to the internet.
- If your phone supports it, use biometrics (fingerprint or face recognition) to increase security and reduce the need for Pins and passwords.
- Enable 'Stolen Device Protection' on Apple devices to restrict or delay what can be done on your device when it is not at your familiar locations.

More hints and tips

- NEVER click on a link or attachment sent from an email address or phone number that you don't recognise even if it was forwarded from someone you know.
- Be especially wary of emails and texts from Banks and Insurance companies especially if they ask to re-verify your credentials.
 - if in doubt ignore them, a genuine Bank will find another way of contacting you.
- Be wary of any sites or callers that ask for the entire password or PIN in financial transactions.

Software updates

- Always keep your software up to date;
 - Windows and MAC OSX usually update automatically, but phones often need you to do something
 - Browsers (Explorer, Chrome, Safari etc.) usually update automatically
 - Anti Virus usually updates automatically – It's essential that you have one on a PC (search. AVG free), less so on phone/tablet though this will change.

Beware of offerings to 'fix' your PC

- There have been many reports of scammers pretending to be Microsoft or BT calling to offer to help you speed up your PC or 'fix' it.
- These are always BOGUS, just politely hang up.
- NEVER let ANYONE instruct you to install software, especially if it lets them control your PC e.g. TeamViewer

Questions

Mendlesham Computer Club

By Giles Godart-Brown

Extra slides

Encryption

Mendlesham Computer Club

By Giles Godart-Brown

Let's have a go at code breaking

IFMMP UP FWFSZPOF

_ E _ _ _ _ _ _ _ E E _ _ _ _ _ E

_ ELL _ _ _ _ E E _ _ _ _ _ E

HELLO TO EVERYONE

Symmetric encryption

- This is called Rotation-1 (rot-1) encoding.
- A code book would look like this; A=B B=C etc.
- This mechanism was improved by having random associations rather than simple rotation and a code book with one page per day e.g. On the 10th January 2025 - A=Q B=N etc.
- This is called symmetric encryption because the same key is used to encrypt and decrypt.
- The Enigma machine added a level of complexity to symmetric encoding by changing the encryption after each letter, e.g. AA may be encoded as HY, it also eliminated the code book.

What's wrong with symmetric encryption ?

- Everyone who wants to decrypt the message has the same key, if someone was to leak the key and say put it on the internet, everyone can decrypt the message. This was a big problem with early pay TV systems with hackers publishing the keys and cloning the set top boxes.
- Whitfield Diffie and Martin Hellman invented Asymmetric encryption where one key is used to encrypt a message and a different key is used to decrypt it.
- The sender of the message has a Public key they share with all recipients. Each recipient has their own unique Private Key. How this works is fiendishly complicated and involves several messages between the recipient and the sender before the message can be decrypted.

What do keys and certificates look like?

Certificate

```

MIIGkDCCBhigAwIBAgIRAP9bf/aQe6ieMG/
1TSIJ60AwDQYJKoZIhvcNAQEMBAQwSzlMAkGA1UEBhMCQVQxEDAQOBgNVBAoTB1plcm9TU0wXKjAoBgNVBAMTIVplcm9TU0wUINBIE
RvbWpfbtBTZWN1cmUgU2l0ZSBDQTAeFw0yMzA5MTkwMDAwMDBaFw0yMzE5MTYyMzU0NTIwMzA5MDAwMDAaBgNVBAMTE2RlYmVuaGFtc
2hZlZC5vcmdudWswgEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDDn+3JAcEHLpLh3nw5TYRgBrkjy3qZ2MEUvbgNpFKfE+aQM
kF1vc1MABn3K4k0X2eqOQ+CU8vEeocTPNYHUtGNbe0vjfcSHhVbZnjd87Ri0PDo017F1yrPao12F54y7WP/2h9e2FuxhmoCTgDa2PXypn/
2h3avydmKFyJTngsIDAAsCRc8RorInj7exZUXiBIIlSczxDuATylyf0Je0Go76e8lktvl+XR1VtkN42pV0nP3IamUAY2jJgyg1YYDlbgwXWENRpWyzATq
S4pj861Sw+WDUMUldoKa+9fc7d+hx+IqB6bIHsEzQLEA4+
+TrTMy8oJswHu6zOLFw7CEnWWHLAgMBAAGjggKaMIIcljAfBgNVHSMEGDAWgBTI2XhootkZaNU9ct5fCj7ctYaGpjAdBgNVHQ4EFgQUNE
OT544mBRFqjdPCCahE3X34Q8lwDgYDVR0PAQH/BAQDAgWgMAwGA1UdEwEB/
wQCMAAwHQYDVR0IBBYwFAIKwYBBQUHAWEGCCSQAQUFBwMCMekGA1UdIARCMEEAwNAYLkwyBBAGyMQECAk4wJTajBggrBgEFBQCC
ARYXaHR0cHM6Ly9zZWN0aWdvLmNvbS9DUFMwCAYGZ4EMAQIBMIGBggrBgEFBQcBAQR8MHowSwYIKwYBBQUHMAKGP2h0dHA6Ly9
6ZXJvc3NsLmNydC5zZWN0aWdvLmNvbS9aZjVU1NMUINBRG9tYWluU2VjdXJlU2l0ZUNBLmNydDARBggrBgEFBQcwAYYfaHR0cDovL3plc
m9zc2wub2Nzc5zZWN0aWdvLmNvbTCCAAQYGCisGAQQB1nkCBAIEGfcEgQA8gB3AK33vvp/
xDli509nB4+GGq0Zylz7EMJmQFhjTr3IKKAAABiqRPZIAAAQDAEgwRgIhAIOUYHrN612J2dYa5Z5mQVHSD64GligEVGjEKbDzSVmsAiEA+ck
g0aH3TKHXw/PdXw9dzYPlnf+
+cwpHjGCKY4+lzvsAdwB6MoxU2LcttiDqOOBShumEFnAyE4VNO9IrwTpXo1LrUgAAAYqskT36AAAEAwBIMEYCIQcNeEoMuwqBOhglOcbD
ziGwhRnlCdiyEJ4zm20Sboa6KghAOuWSEnF9FXMWWw+sfJkwOgZCzrucfn4Pmel32ZLNslLqMdcGA1UdEQQwMCC6E2RlYmVuaGFtc2hZlZC5
vcmdudWuCF3d3dy5kZWJlbnhhbXNoZWQub3JnLnVrMA0GCSqGSIb3DQEBAQUAA4CAQAKJ9zdY5P5xcrG1hp/3p/
9Rk64YF9YzaDlf8RI5upCdeVz4qVq/
AkOdhHy19eq7i30mquF8zWvJTqk2FzEeb6wOiv9y9qU8yhfhBER8UAdfGzpnxazao9ksn+AMB5hx4LXE2+akysxlO3ftpOmlatV3cOlmlAY5nx
bS/evcOr9U5+Ln7MgCL9C+49Hbtz260FFXNTMd3FCg+1nzYY/+Zwfx5qdadof3ItzMyz/HBy/GrUePTGUNwff66EdUHVt/
bAltB6vEnPMzBjKcO0BXsAjcPbgncV20lxcD9JvTDV9F2AhxvlpRV0kfsH/
QY4YRrv+Uj6LEwZB4hNooKpMKdr8wvNrb0Edr7i2OcXAUe5GzRxfu0KPFbXTU+AadfaVeMS4SQuv/
cJUGR3DBuT12DDGzQuCjUJBRK3IGUoUjyGTHZQNme1SepXmZCyZ6Dv+qqrYs21TlSLuKAnlIC8Zz3GV3FoniSBpuA7DntbmqzpoE/
hrhctupNrSL2vgyqt52FisnG91j6Um3EL2d90p9DQKzUx73sGMC4tTVYnB44PLZTKvK0l6Zf8s0dlvwBWqVktCz4c65Vu//
Jw7auWDH2xMAZrybjfD0Ye2wnzqzjPHgEC0D3opbh4AUESvfk6P1Ls/NaxiwXVPEMiGWTilNpr3mNvv34U/w0BYkg==
    
```

Key

```

MIIEPgIBAAKCAQEAw5/
tyQHBBYKS7B958OU2EYAA5I8t6mdjBFL24DaRSnxPmkDJBdb3NTAAZ9yuuNF9nqjkPglPLxHqHLTzWB1LrjW3tL433Lkh4VW2Z43FO
0YtDw6NNexdcqzxkNdheeeMu1j/9ofXthbsYZqAk4A2tj12KZ/
9od2r8nZihciU54LCAwLAKXPdqDY+3sVWF4gSjUgs8Q7gE8pWH9CXtBqO+nvJZLbyPI0dVbZDeNqVdJz9yGplAGNoyYMoNwGA5
W8IF1hDUaVsswE6kuKY/
OtUsPlgzFDCHaCmVvX3O3focfagem5R7BM0CxAOPvk60zMvKCUsb7usizxcOwhu1lhywIDAQABAoIBAQRwi3NLuZf542qKgWty2
OOHHEFC/y84gzvQtU31tBHhU/
kfr9e+5xxG353dxJlnS0KaPOHZqtvsIIRjYewwAat9Azb9jqBwBwVko5V58FJ7elzGFCR4IcS6VUpVEKxKwU67SPAzhOVU0tKf7Bmta
eN/psUhmTV/jBhtZbQcNmMo7sIXv+JEaee9DZoSaMPXhVLVAR3XdsPT6t6sBmlwU9BkNZ4u6RhHe/
ISDcUROVQMSykb9ZFTLpOb8/pOqw365mlbY35rdIDMNUgy5mJlVw59LZ6FLzeo4YjS9UZ4mVYH86hVkr3Om4cqDJHECC095/
Ayn3NgbEoVsiOQvdO1BAoGBAP5+9OV6GpZftVly27ewm7KIY0A/
tLrrhOf05bXRmtbC3sBw3tNary6QkCbhVq0i+NDyPSIY2A84D3YQQPabqjBecwKHaQpYsFcpLjcQio+f9m2zvHIN4ZlmybD5gfz3q/
pDbdw7chkkUqV2Z7KIYH2sw8TJ1E19eK2McWzHqhAoGBAMTH5vRRVYAGz0kWCzmE2NWKQki7jQRAIWKsu+blWA3Xxqav5fh
MXrhwmqTza5zPNIfvg0KButwGoGCGrEiVdZYKBhW1BWZiyOknNXfWSP29ibvwT1aIAXdC8O0ycCbR8HWryskrW4UbjJc9QFWwE
3IHw6rEk1vfyadsowtDrAoGBAL6oyjuo8IY7gbZuJcGzhryNffkvB7loi290S4Y0HTOMb9tLhNe5Nf/
R4pSypb13qV1HiSN5kmlEblDcyG54S/
eu8LyisCydfLiz+Uvs5zf0HcAxOBQEz0Yw2tt947WNhAVxqa8GUX3RqerVlkaHs5Yzei7RrdWn7GLIVqISJBAoGBAI+/
xExn+gClePNYAhoJmc7ssBh4LuvDW9ExxCoig+2g2gl8T9rBbbjpn4+cx10P27dX7trRn1pwSzyeUWdiwLFTMH8PNuEMiGMiRlvKS/
EE4K5y6IQsCvLdH0edGzebd6D3dVE3GuZWtZxGaC5xNAvzOjv1BmrA727DNoJGC/
AoGBAJwYUQ+DhfrkkCj0v4N4pSHFBCm7RXhtt02dfnk2cq2sW8J4CqblDJMhzPFXvY8NHo6yUhxTdh4tGJjqhOV37rhu/
ryltr9aLxLeJw37GLSpGWUl55EOZtZ09nz00DUTKEVn08EvgNmLnhGf26wyaj8Ml4+SmJc/GgKy7eu8y
    
```

The Maths for these is VERY complicated

$$H(s) = \frac{1}{1 + \underbrace{\frac{RC(m+1/m)}{n}}_{\frac{2\zeta}{\omega_0} = \frac{1}{\omega_0 Q}} s + \underbrace{R^2 C^2}_{\frac{1}{\omega_0^2}} s^2},$$

How do I make sure the site is secure?

- Sites that have valid certificates and use encryption use the Secure Socket Layer (SSL) to protect messages.
- Never put personal details into a site which starts with http rather than **https** – s means secure! Look for the padlock.



These sites encrypt all messages

Examples

<http://example.com>

<https://example.com>

What is a virus?

What is a virus?

- Wikipedia definition:
“A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. If this replication succeeds, the affected areas are then said to be "infected" with a computer virus”
- Strictly speaking it's a virus only if it gets itself buried into a host program (e.g. Microsoft Mail) if it runs on its own it is called a Worm
- People create viruses for a number of reasons, profit (e.g. ransomware where it demands payment to restore your computer), political power, to demonstrate a vulnerability of a product, corporate gain, or just plain devilment.

A VERY simple virus example

- A simple program to print “Hello Mendlesham”
 - `print ("Hello Mendlesham");`
- Now with a virus
 - `print ("Hello Mendlesham");`
the next line will delete your windows directory rendering your computer useless
`rmdir "C:/Windows";`
- Typically, they are much more complex than this and include mechanisms for infecting other computers

Are you being tracked?

Do I need a Virtual Private Network (VPN)

- There are a lot of adverts on the TV trying to scare you into buying a VPN (NordVPN, Norton).
- They prey on the fact that:
 1. You need to encrypt ALL of your Internet traffic.
 2. You need to avoid 'Trackers'
 3. Your location can be accurately tracked
- This is overkill for regular consumers because;
 1. Most internet traffic is already encrypted (urls that start with https)
 2. Browsers with Ad blockers prevent trackers
 3. The physical location is pretty inaccurate for all but your permitted Phone apps

AD blockers

- You can prevent trackers from bombarding you with Ads by using an AD blocker that prevents these malicious pop-ups. Mine has currently blocked 492,306 ads.
- The most popular AD blocker for Chrome users is called Adblock and can be installed from <https://chromewebstore.google.com/detail/adblock>
- There are also Ad blockers for phones and tablets (search the App Store)
- Note some web sites detect you are using an AD blocker and will ask you to disable it. In nearly all cases there is another web site you can use that works with the AD blocker (back to a Google search)

Application Tracking

- On a Phone or Tablet you may be asked to allow the app to track your location so they can send you more tailored ads.
- I would only allow this for apps that need to know where I am e.g. fitness trackers, and then I would only allow it when using the App, if this makes sense.
- A notable exception is device trackers like Tile.

Two Factor Authentication

Mendlesham Computer Club

By Giles Godart-Brown

What is 2-Factor Authentication ?

- 2 Factor Authentication (sometimes called Multi Factor Authentication or MFA) is based on “something you know (a password) and something you own (a mobile phone or email account)” thus doubling the security of the connection. Increasingly web sites that involve a financial transaction or private data will implement this.
- How it works
 - When you register on a web site, in addition to your password, you also register your email address and mobile phone number.
 - When you log into the site, it first asks for your password (factor 1), then sends you a text or email.
 - The text or email contains a code (usually a 6 digit number) that you must enter into the web site in order to log on. This confirms that whoever is logging in also has your mobile phone (factor 2).
- If you are in an area with poor mobile coverage, some sites allow you to specify an email address instead of mobile number. If you get a new phone, don't forget to update the number on the web sites that use it.

Conclusion

By Giles Godart-Brown

The internet is not intrinsically unsafe

Of the trillions of users of the WWW, very few are compromised, just be 'Web Savvy'



<https://www.avg.com/en-gb/free-antivirus-download>

Sharing Passwords

Mendlesham Computer Club

By Giles Godart-Brown

Sharing Passwords

- Do not send passwords in unencrypted methods
- The following are encrypted
 - WhatsApp and iMessage , but beware who you are sending to
 - Text is still pretty safe