

Topic Outline

Sources of information

Online Intrusion Threats

Website data breaches

Scams and Fraud

Defences

Authentication and Password security

Windows security

Network security

Online security (banking, purchasing etc.)

Sending documents securely

Public WiFi

Privacy concerns

Social media and privacy

Data backup

Short Excerpt from 4-Corners program “Cyber War”, 29-August 2016

<http://www.youtube.com/watch?v=SMs5DVILK8E>

Useful Links for more Information

Protecting yourself online – What everyone needs to know (PDF booklet)

www.ag.gov.au

Stay Smart Online (Aus. Govt) – subscribe to alerts.

www.staysmartonline.gov.au

Scam Watch

www.scamwatch.gov.au

Australian Cyber Security Centre

<https://acsc.gov.au>

Ask Leo – subscribe to regular newsletter. Excellent source of information, particularly relevant to Windows.

askleo.com

How to Geek (more a source of knowledge than security advice)

www.howtogeek.com

Online Intrusion Threats

Malware – general term for all malicious software.

Keylogger - malware that records your keystrokes, e.g. passwords.

Trojan - backdoor that allows unauthorised external access. May be used to create a botnet.

Virus - propagates and destroys.

Spyware – steals information from host computer.

Phishing – a fake website that emulates a legitimate site, e.g. a bank, to steal passwords.

Ransomware – encrypts data files and demands payment.

Spam – unsolicited email advertising - may carry malware payload.

Identity Theft and Financial Fraud – a possible consequence of poor privacy practices.

Internet of Things (IoT) – many electronic devices now connect and have poor security.

Foistware – unwanted software installed along with a legitimate package.

Browser exploit – malicious code that exploits a browser vulnerability.

O/S exploit - malicious code that exploits an operating system vulnerability, e.g. Windows.

Scams – attempts to extract money by various means.

Drive-by download – links on websites that aren't what they seem.

Ransomware

Ransomware is a virus that encrypts your data files so that they can't be read. Typically acquired by clicking on an email link, e.g. fake AusPost delivery message. It will demand that you pay money (a "ransom") to get access to your PC or files.



“Wanna Cry 2”
ransomware attack,
May 2017

Ransomware (cont.)

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

XUNjNx-pKazyd-gK2GcG-JLP8uT-fcY2hY-zJo3PX-KQU8ga-65FSWj-Q423Nc-CoCgaZ

If you already purchased your key, please enter it below.

Key: _

“Petya” ransomware 28 June 2017.
Spread via a Word Macro attached to email. It appears that only older unpatched versions of Windows were affected.

Ransomware (cont.)

Defences:

- Don't click on email links or attachments unless absolutely sure they are safe.
- Ensure you have anti-virus software installed and up-to-date (not 100% effective).
- Ensure the latest operating system updates are applied.
- Use a modern browser with an ad-blocker plugin.
- Use a Standard user login in Windows, not Administrator.
- Backup, Backup, Backup! (and keep an offline copy).

Ransomware (cont.)

Recovery:

If possible, remove the virus and recover your files from backup.

or

Re-install Windows – all data on main drives will be lost.

More info:

[Microsoft Malware Protection Center](#)

Phishing

Phishing is a form of fraud in which the attacker tries to acquire confidential information such as login credentials, account information, or credit card numbers by masquerading as a reputable company.

A typical example would involve a phony website link sent by email, SMS, social media or other messaging service that transfers to a fake version of a legitimate entity's website, e.g. a bank.

When you login, they acquire your password for the real site.

Example of a phony link:
www.westpac.com.au

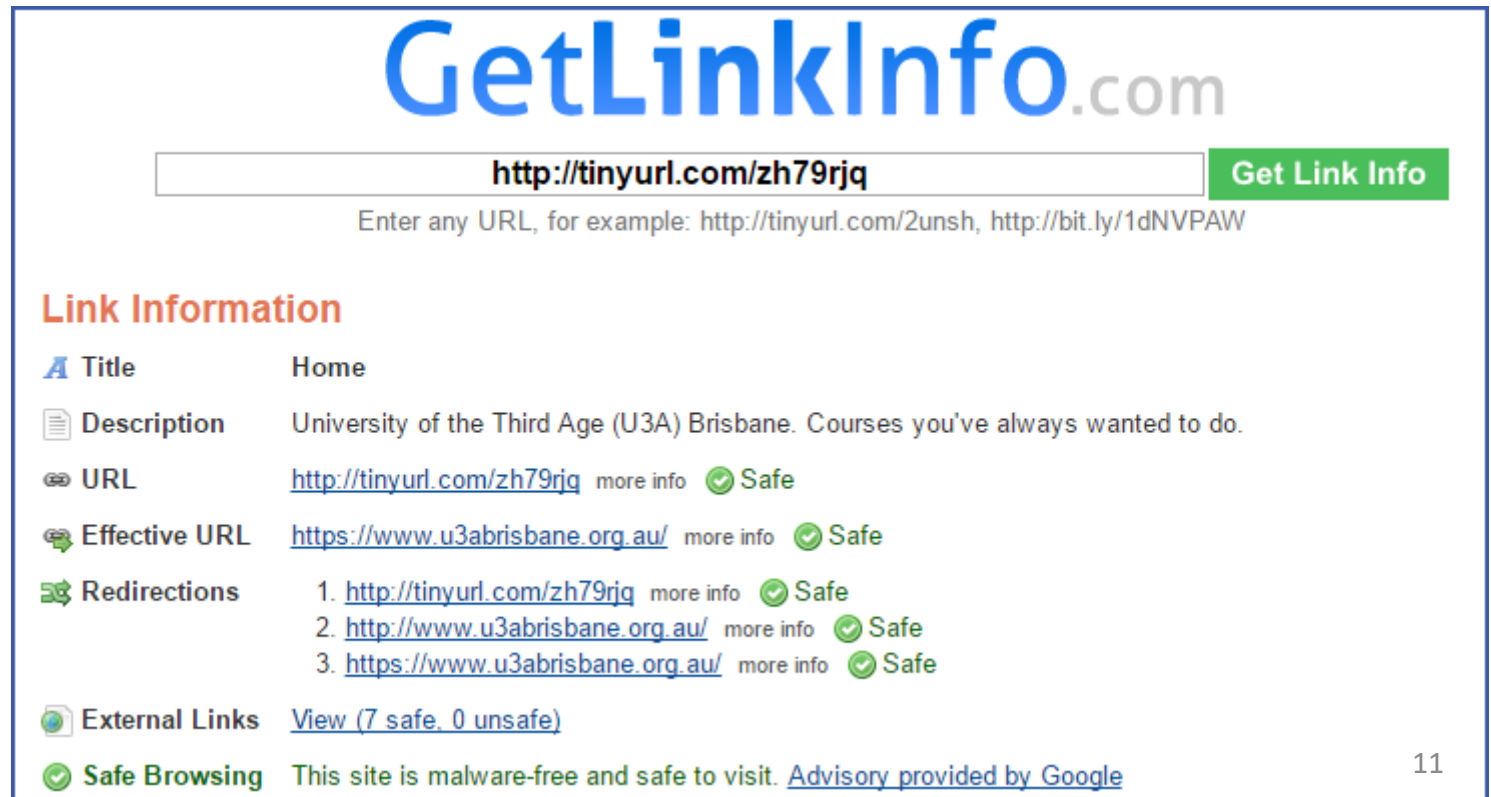


Phishing – don't get hooked





Be suspicious of requests to verify or confirm your login details. Reputable institutions don't operate in this way.

Check the actual URL of any link by hovering over it, or checking the URL in the browser address bar.

Use a service such as www.getlinkinfo.com to decode an obscure URL:



The screenshot shows the GetLinkInfo.com interface. At the top, the URL <http://tinyurl.com/zh79rjq> is entered into a search box, with a green 'Get Link Info' button to its right. Below the search box, a text prompt reads: 'Enter any URL, for example: http://tinyurl.com/2unsh, http://bit.ly/1dNVPaw'. The main content area is titled 'Link Information' and lists several details:

- Title:** Home
- Description:** University of the Third Age (U3A) Brisbane. Courses you've always wanted to do.
- URL:** <http://tinyurl.com/zh79rjq> more info  Safe
- Effective URL:** <https://www.u3abrisbane.org.au/> more info  Safe
- Redirections:**
 - <http://tinyurl.com/zh79rjq> more info  Safe
 - <http://www.u3abrisbane.org.au/> more info  Safe
 - <https://www.u3abrisbane.org.au/> more info  Safe
- External Links:** [View \(7 safe, 0 unsafe\)](#)
- Safe Browsing:** This site is malware-free and safe to visit. [Advisory provided by Google](#)

Try the Phishing Quiz

www.opendns.com/phishing-quiz


The image shows a browser window displaying a phishing page for American Airlines. The address bar shows the URL `http://www.aa.airlinesaamemeber.com/login.php`. Two callout boxes provide educational information:

- 2 No "https."** The real American Airlines login page will always use "https" indicating a secure login.
- 1 Forged URL.** Even though `aa.com` is the real domain for American Airlines, the actual domain for this phish is `airlinesaamemeber.com`.

The page content includes a navigation menu on the left, a "To login:" section with instructions, and a "Login" form with fields for AAdvantage Number and Password, along with checkboxes for "Remember My AAdvantage Number" and "This is a public/shared computer, do not remember me." A "GO" button is present at the bottom right of the form.

Example fake email:

From: WestPac <infos@westpac.com.au>
Subject: Notification
Date: 23 May 2013 11:44:33 AM AEST
To: undisclosed-recipients;



Thank you for banking online at **Westpac**, your security is our primary concern against the recent spate of fraud and identity theft involving online account holders. We have introduced additional security measures and upgraded our software to protect our customers.

The security upgrade will be effective immediately and requires our customers to update their access and Sign in Protection activation.

[Please Upgrade Your Information](#)

Warning sign: 'P' in Westpac is capitalised. If this was an official email, this would unlikely be sent with such an error.

Warning sign: Recipient address is undisclosed and/or not your own. There is also no other form of personalisation.

Warning sign: It's unlikely you would need to log into an account to have software security upgraded or activated.

Warning sign: grammar and capitalisation errors. What does "Sign in Protection activation" mean?

DONT CLICK! When in doubt, try rolling over the link to reveal its true destination. In this case it links to a phishing site:
<http://alternabtl.com/wp/index.html>

Website data breaches

Some well-known examples:

Yahoo 2014 (announced Sep 2016) – 500 million accounts compromised.

MySpace – 300 million accounts.

LinkedIn 2012 – 165 million accounts.

Dropbox 2012 – 68 million accounts.

Adobe 2013 – 152 million accounts.

How does this happen? – inadequate website security.

What should affected users do? – change password, use secure passwords, be cautious if asked to provide personal information.

Typically the data stolen is email addresses, encrypted passwords, encrypted credit card details, and other personal information.

Encrypted data is at risk if it can be decrypted by a “brute force” attack by the hacker.

Have your details been compromised?

This site tracks and records accounts that have been compromised. This is a legitimate site that trawls data that has been published by hackers:

Have I been Pwned? (owned)

<https://haveibeenpwned.com>

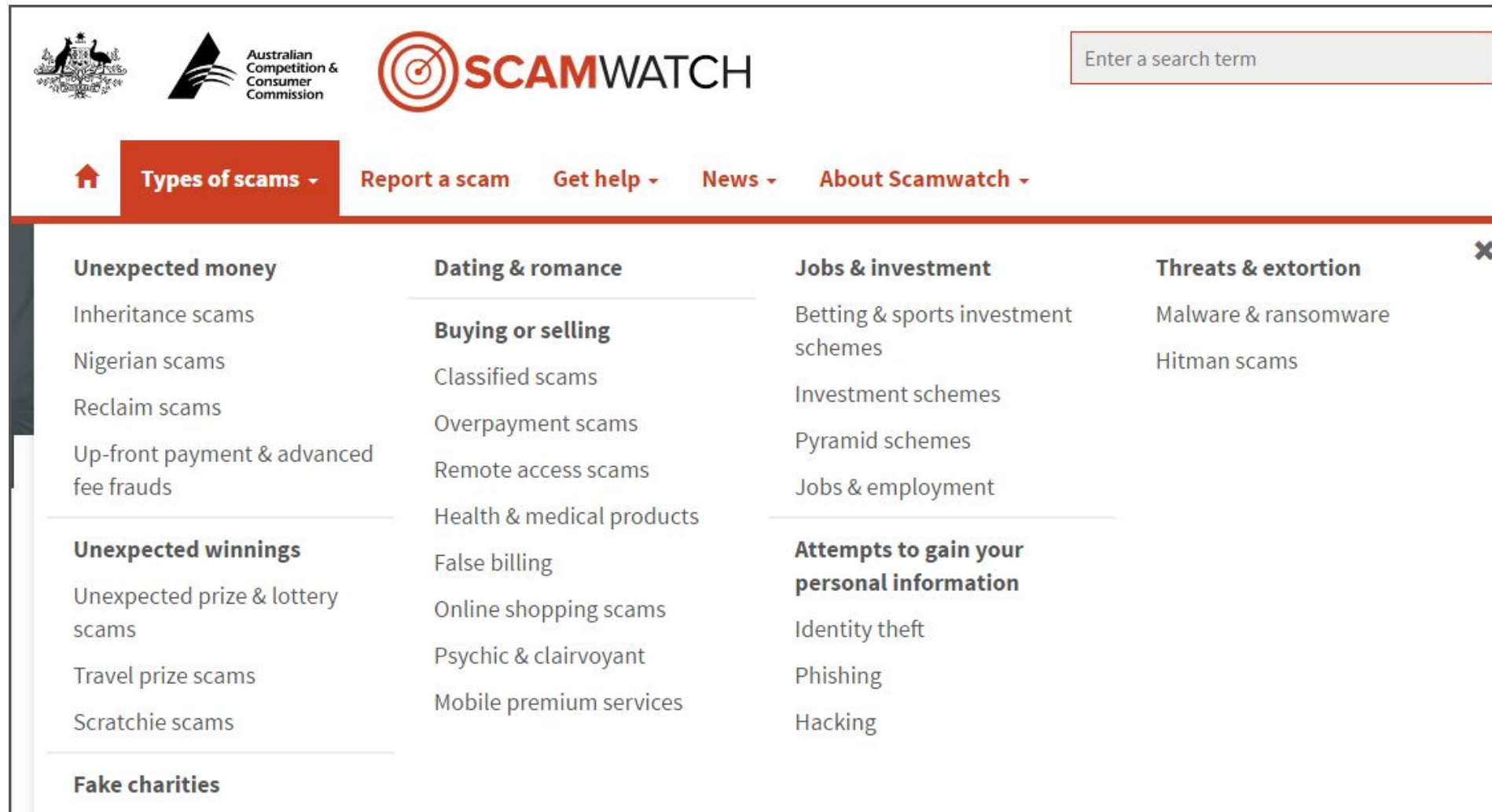
If your email address is listed, you should change your password at the named website.

More info on sites breached:

<https://haveibeenpwned.com/PwnedWebsites>

Scams

www.scamwatch.gov.au



The screenshot shows the Scamwatch website interface. At the top left are the Australian Coat of Arms and the Australian Competition & Consumer Commission logo. To the right is the SCAMWATCH logo, which features a target icon. A search bar is located in the top right corner with the placeholder text "Enter a search term". Below the logo is a navigation menu with a home icon, "Types of scams" (highlighted in red), "Report a scam", "Get help", "News", and "About Scamwatch". The main content area is a grid of scam categories, each with a title and a list of specific scam types. A close button (X) is visible in the top right corner of the grid.

Unexpected money	Dating & romance	Jobs & investment	Threats & extortion
<ul style="list-style-type: none">Inheritance scamsNigerian scamsReclaim scamsUp-front payment & advanced fee frauds	<ul style="list-style-type: none">Buying or sellingClassified scamsOverpayment scamsRemote access scamsHealth & medical productsFalse billingOnline shopping scamsPsychic & clairvoyantMobile premium services	<ul style="list-style-type: none">Betting & sports investment schemesInvestment schemesPyramid schemesJobs & employment	<ul style="list-style-type: none">Malware & ransomwareHitman scams
<ul style="list-style-type: none">Unexpected winningsUnexpected prize & lottery scamsTravel prize scamsScratchie scams		<ul style="list-style-type: none">Attempts to gain your personal informationIdentity theftPhishingHacking	
<ul style="list-style-type: none">Fake charities			

Some example scams

ATO tax scam (phone call)

[Steer clear of tax scams](#) (*ScamWatch* July 2016)

Recorded message says tax is overdue, letters returned unopened, arrest warrant issued and police on their way. Caller has taxpayer's name and address and an 02 phone number is given.

(Personal details probably obtained from an online source).

Note: Australian phone numbers easily faked with VoIP.

Tech Support scam (phone call)

Caller claims to be from Microsoft, saying there is a problem with your computer. They request you allow remote access to fix.

Defences

Adopt Critical Thinking (healthy scepticism), i.e. don't be gullible.

Be aware of risks.

Protect personal information.

Think before clicking on any link, or opening any attachment!

Software Defences

Anti-Virus (Activate *Windows Defender* if you have no 3rd party product).

Anti-Malware (*MalwareBytes*).

Windows Firewall (built-in).

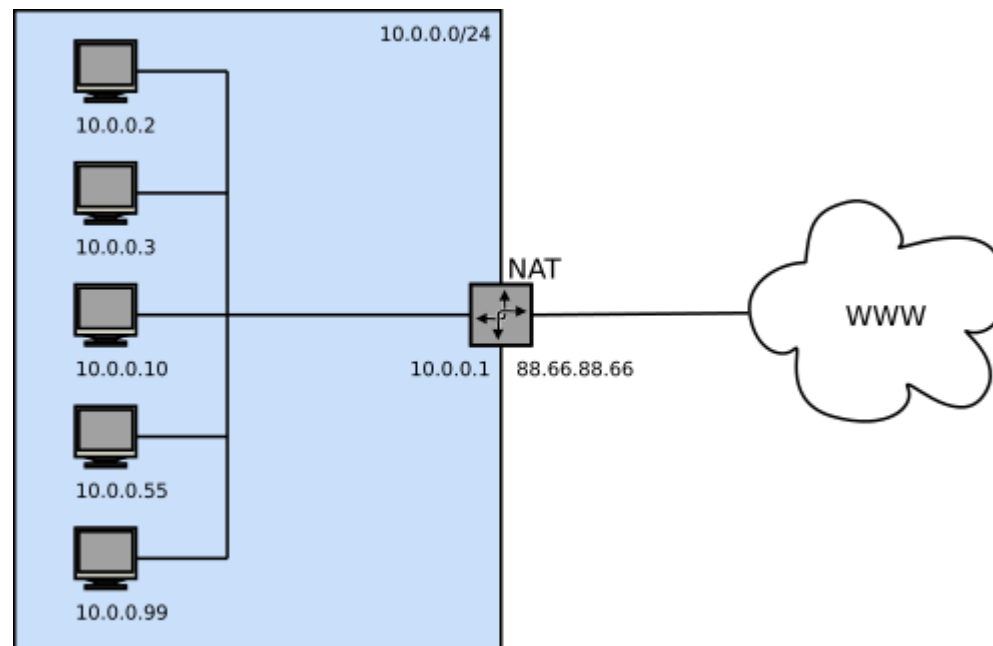
Backup (*Windows Backup, Genie Timeline, Macrium Reflect*).

Hardware defences (home broadband)

Router/modem configuration

- Disable remote access (may be turned on by default!)
- Change default admin password.
- Configure firewall port blocking (requires some technical expertise)
- Use strong WiFi password and encryption (Select WPA2 encryption)

Note: Home routers provide a natural firewall through Network Address Translation (NAT).



WiFi Security

Good security

Home WiFi with a strong WiFi password and WPA2 protocol.

If you have no password or weak encryption (e.g. WEP) others can access your internal network.

Mediocre security

Public WiFi hotspot where a password is required for access.

Password ensures that data is uniquely encrypted between your device and the router.

Be aware of the possibility of **fake** hotspots.

Not secure

Public WiFi network with no password.

All transmissions are plain text!

Passwords and authentication

Strong passwords essential

- minimum 10 characters, 12 or more is better.
- Use random characters, upper, lower, numeric, special characters (\$ # % etc.)
- Avoid dictionary words.
- Change regularly (e.g. annually).
- Never use the same password on multiple sites.
- Use a Password Manager.

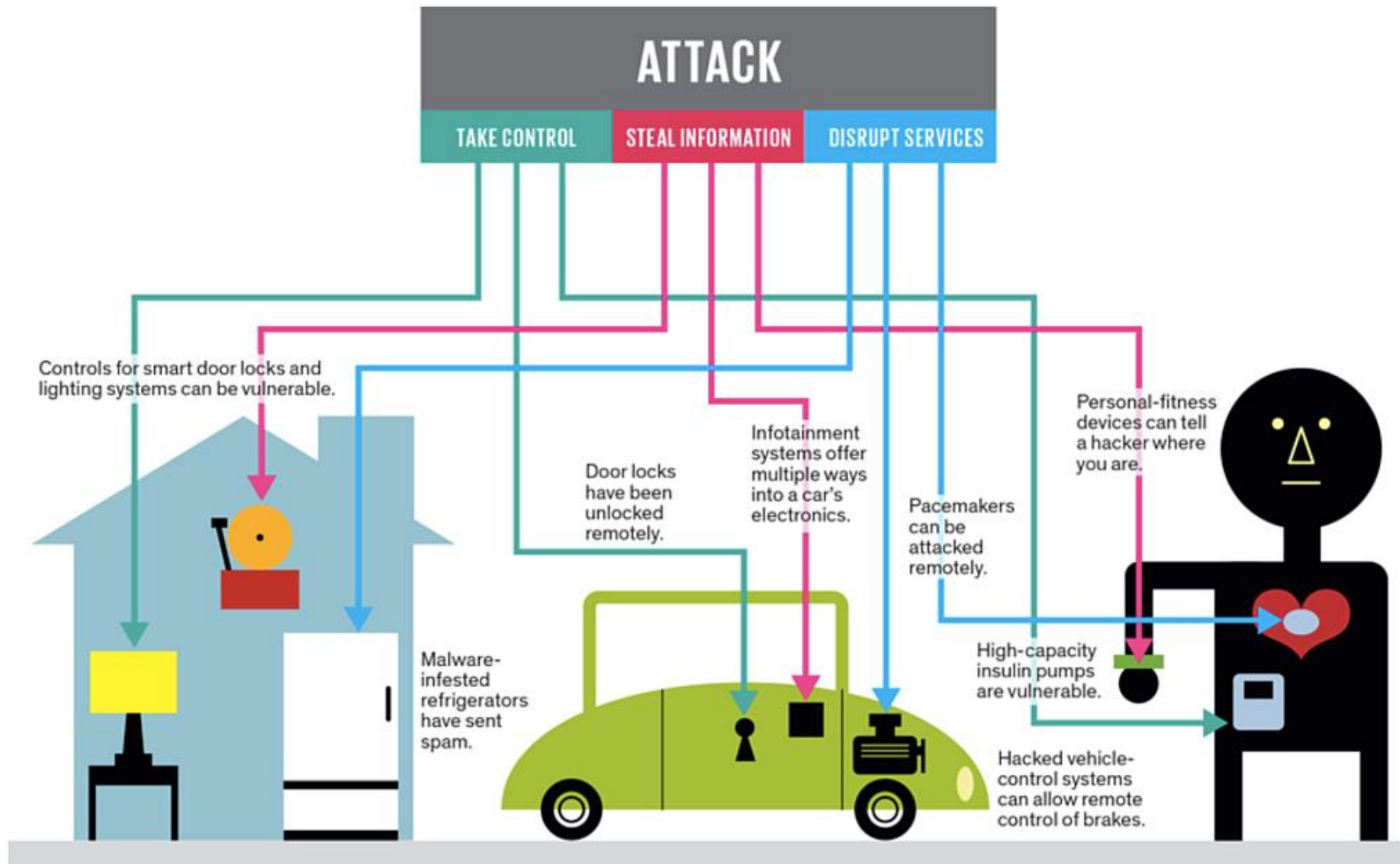
Good password security requires effort!

“As of 2011, available commercial products claim the ability to test up to 2,800,000,000 passwords a second on a standard desktop computer using a high-end graphics processor. Such a device can crack a 10 letter single-case password in one day.”

Source: en.wikipedia.org/wiki/Password_cracking

Internet of Things (IoT)

More and more devices in the home now connect to the Internet, and this will explode in the next few years. Many of these devices have limited security.



Two-Factor Authentication

Two Factor:

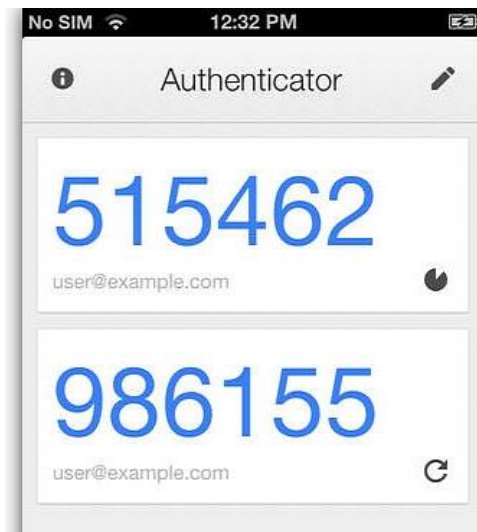
- Something you know (password)
- Something you have (security token, phone)

Provides strong security for critical applications, e.g. banking, email, by requiring entry of a generated number (changes every 30 or 60 seconds).

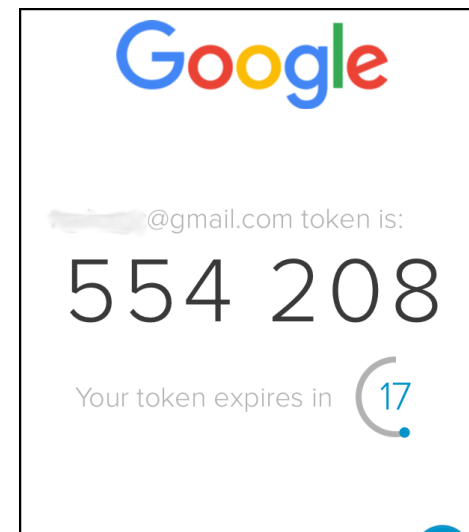
Token



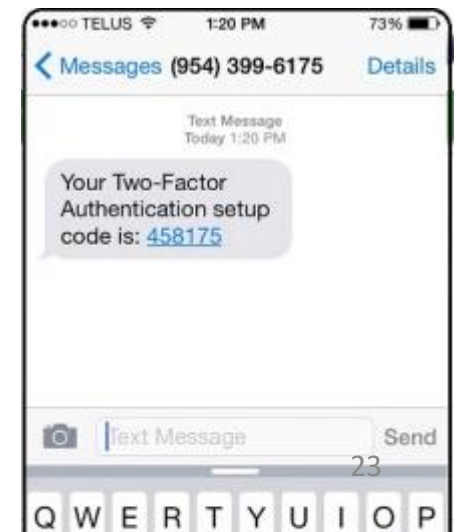
Google Authenticator app



Authy app



SMS message



Two Factor Authentication (cont.)

Sites that offer 2-factor Authentication:

- Banks (token or SMS)
- PayPal (SMS)
- Google/Gmail (*Authy, Google Authenticator* or SMS)
- Facebook (*Authy, Google Authenticator* or SMS)
- Twitter (SMS)
- Dropbox (*Authy, Google Authenticator*)
- Amazon (*Authy, Google Authenticator* or SMS)
- LastPass (*Authy, Google Authenticator* and others)
- and more

More info:

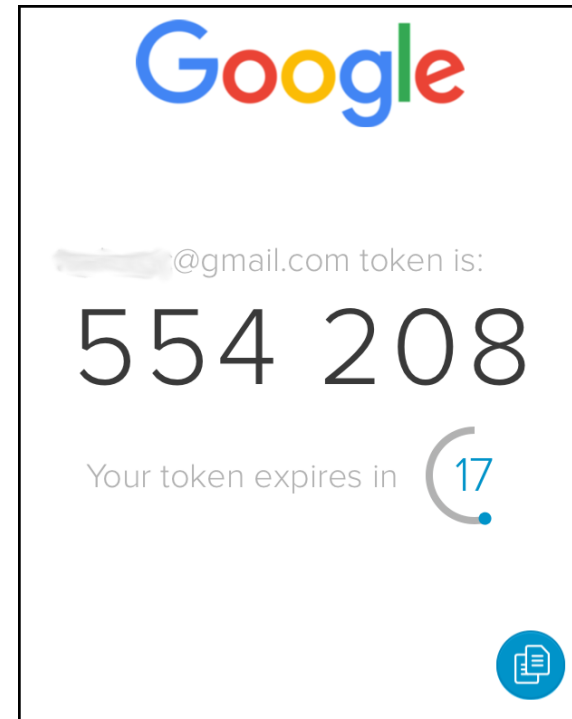
[Here's Everywhere You Should Enable Two-Factor Authentication](#)

Two Factor Authentication (cont.)

Example: Using gmail with *Authy* (phone app)

- Important since Google password also provides access to *Google Drive, Calendar* etc.
- Can be bypassed on computers you frequently use, e.g. home PC.
- Typically used in conjunction with webmail.
- Can also use *Google Authenticator* for the same purpose, but *Authy* is generally regarded as a better product.

The objective is to prevent an unauthorised person from accessing your account using password alone. You can disable it on computers you regularly use, e.g. at home.



Password Managers

Commonly used Password Managers:

Bitdefender (anti-virus package, but includes password manager)

LastPass (browser extension with encrypted remote database)

KeePass

Password Safe

Inbuilt browser password managers are not secure.

Don't use for banks, email etc. since passwords can be retrieved by anyone with access to the computer.

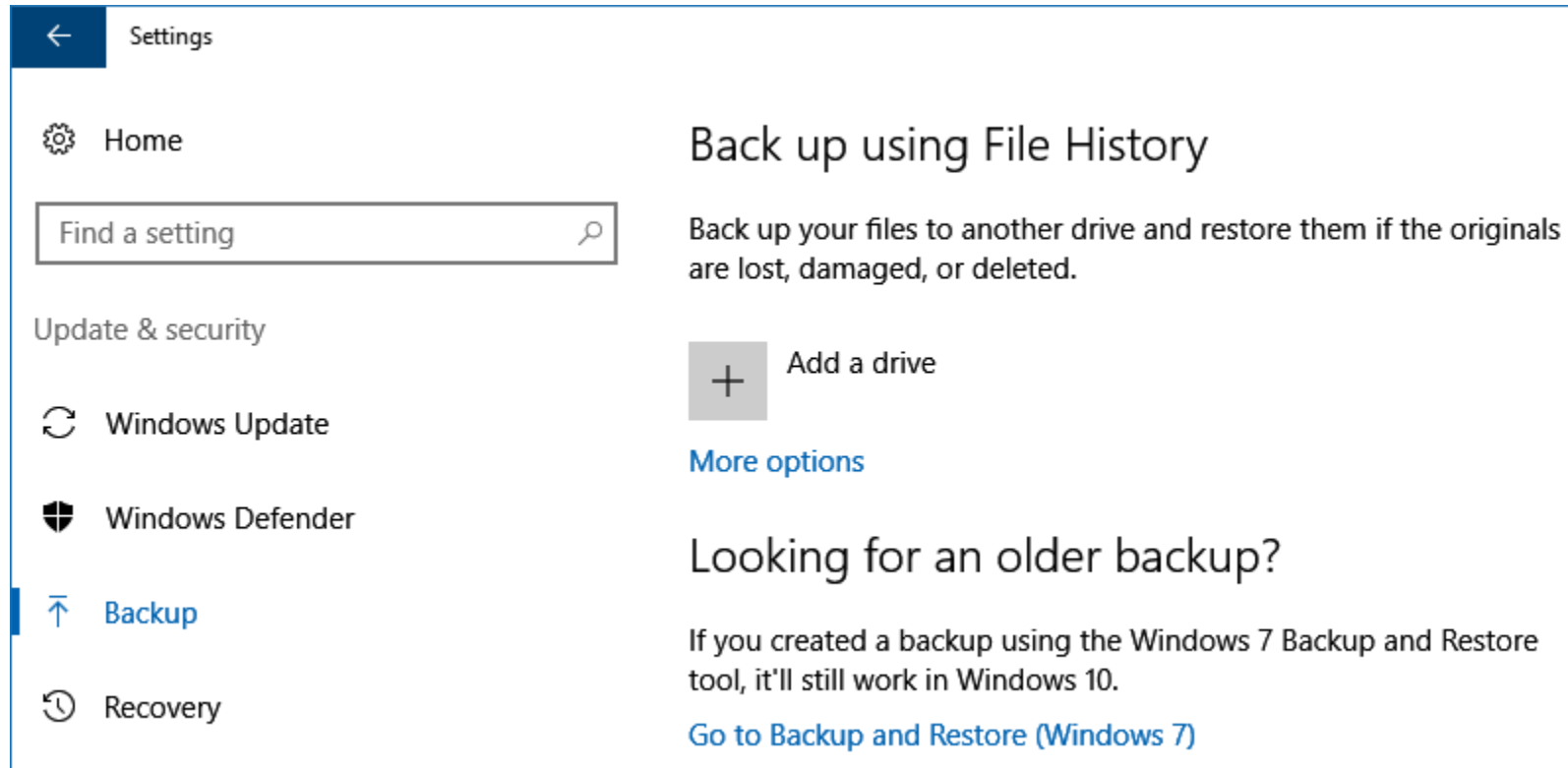
Windows Security

Recommended practices

- Use a Standard account, not Administrator: *Control Panel > User Accounts*
- Update Privacy defaults: *Settings > Privacy* (Turn everything off)
- Change Update defaults: *Settings > Update & security > Advanced options*
- Create Restore Points: *Control Panel > System > System Protection*
- Use an incremental Backup System (*Windows Backup, Macrium Reflect, Genie Timeline*)
- Make an offline backup regularly, i.e. disconnected external drive.
- Use anti-virus (*BitDefender, Windows Defender, AVG, Avast* etc.)
- Check Browser Extensions regularly.
- Consider encrypting sensitive files (*AxCrypt, 7zip*)
- Turn off Remote Assistance: *Control Panel > System > Remote settings*

Windows Backup

Settings > Update & Security > Backup



The screenshot shows the Windows Settings application. The left sidebar is visible with the following items: a back arrow and 'Settings' at the top; 'Home' with a gear icon; a search box containing 'Find a setting'; 'Update & security' as a category; 'Windows Update' with a refresh icon; 'Windows Defender' with a shield icon; 'Backup' with an upward arrow icon and a blue highlight bar; and 'Recovery' with a clock icon. The main content area is titled 'Back up using File History'. Below the title is a descriptive paragraph: 'Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.' There is a button with a plus sign and the text 'Add a drive'. Below that is a link 'More options' in blue. The next section is titled 'Looking for an older backup?' followed by a paragraph: 'If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.' At the bottom of this section is a link 'Go to Backup and Restore (Windows 7)' in blue.

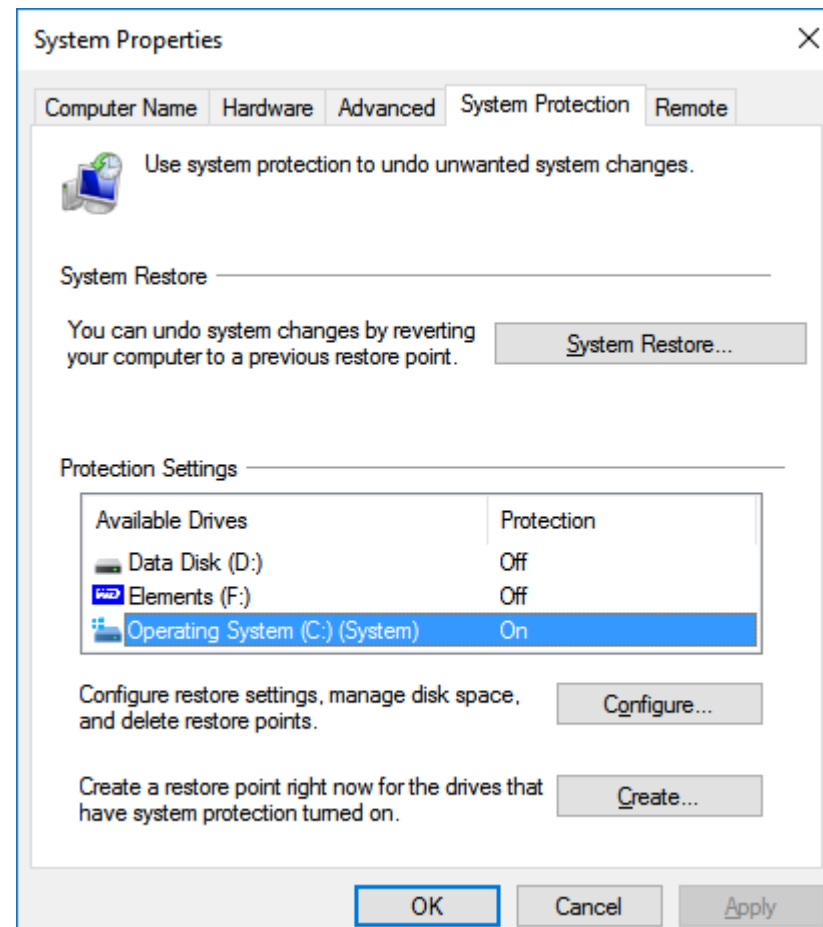
Windows Restore Point

Control Panel > System > System Protection

Windows automatically creates Restore Points before installing software or critical updates.

However, it is advisable to manually create Restore Points from time to time.

If a system error occurs after an update, the Restore Point can be used to return the system to the state it was in before the Update.



Online Banking and Purchasing

- Always use two-factor authentication for online banking.
- Visually check URLs.
- Use PayPal to limit credit card exposure.
- Get a separate debit card for online transactions, with a low limit.
- Only use secure sites (<https://>)
- Banks should preferably have Extended Validation certificates.

Note: There are moves afoot to require most sites to use https, even if not used for financial transactions. Google now flags secure sites and will soon mark all non-https sites as **insecure**.

Online debit card example

Auspost Load&Go Reloadable Visa Prepaid Card

- Buy at any Post Office (\$6.95), register online.
- No credit checks, manage balance online.
- No name on card. Works like any credit card.



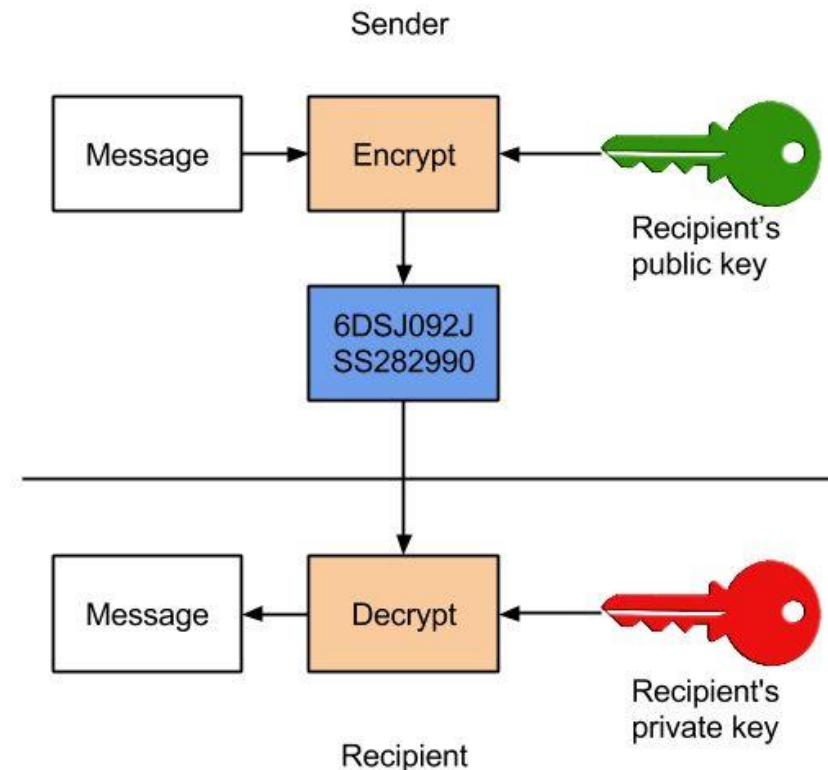
Secure websites: https://

If site URL begins with “https” instead of “http” it means the site is secured using an SSL Certificate.

Data is encrypted end-to-end (between your computer and the remote server) using extremely strong (unbreakable) encryption.

SSL/TLS assures:

- Identity (the real site)
- Confidentiality
- Data Integrity



Cryptography – a controversial history

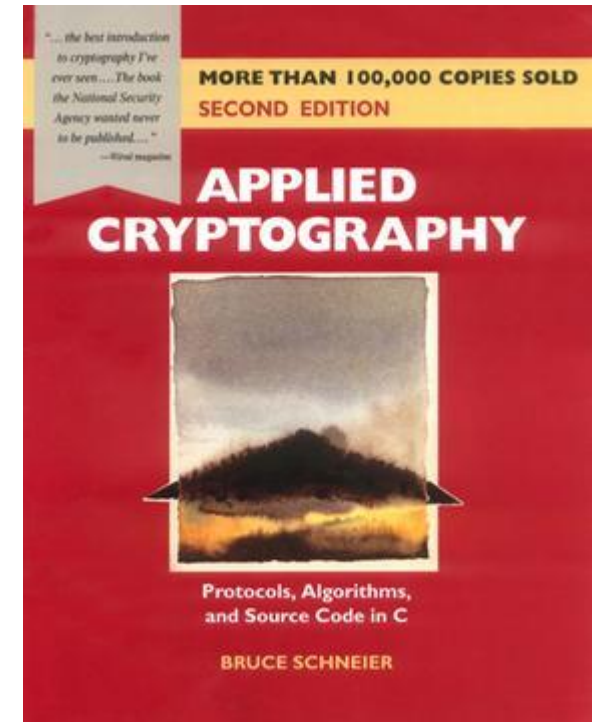
Prior to mid-1970s cryptography was the exclusive preserve of intelligence agencies and the military.

A civilian paper in 1976 revolutionised the field by describing a method for exchanging keys over an open system.

(*Diffie and Hellman* – they later won Turing award - “Nobel Prize” of computing).

First published book: *Applied Cryptography* – Bruce Schneier (1996). (Accompanying CD containing computer source code was banned in Australia.)

Cryptographic products can be subject to strict classification under Defence regulations.

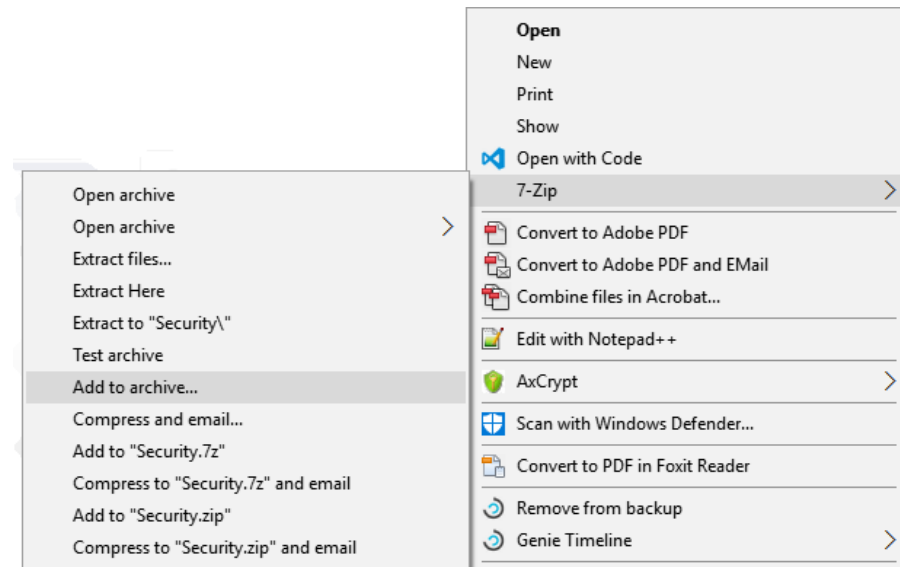


Sending documents securely

Email is inherently insecure and your communications could be read by persons other than the intended recipient. Email is typically sent in plain text, i.e. not encrypted.

If you need to send information securely, e.g. a confidential document, an easy way to do this is by installing [7-zip software](#) (also commonly used to unzip .zip files).

To encrypt a file (as a .zip archive), right-click on the filename in Windows Explorer and select *Add to archive*:

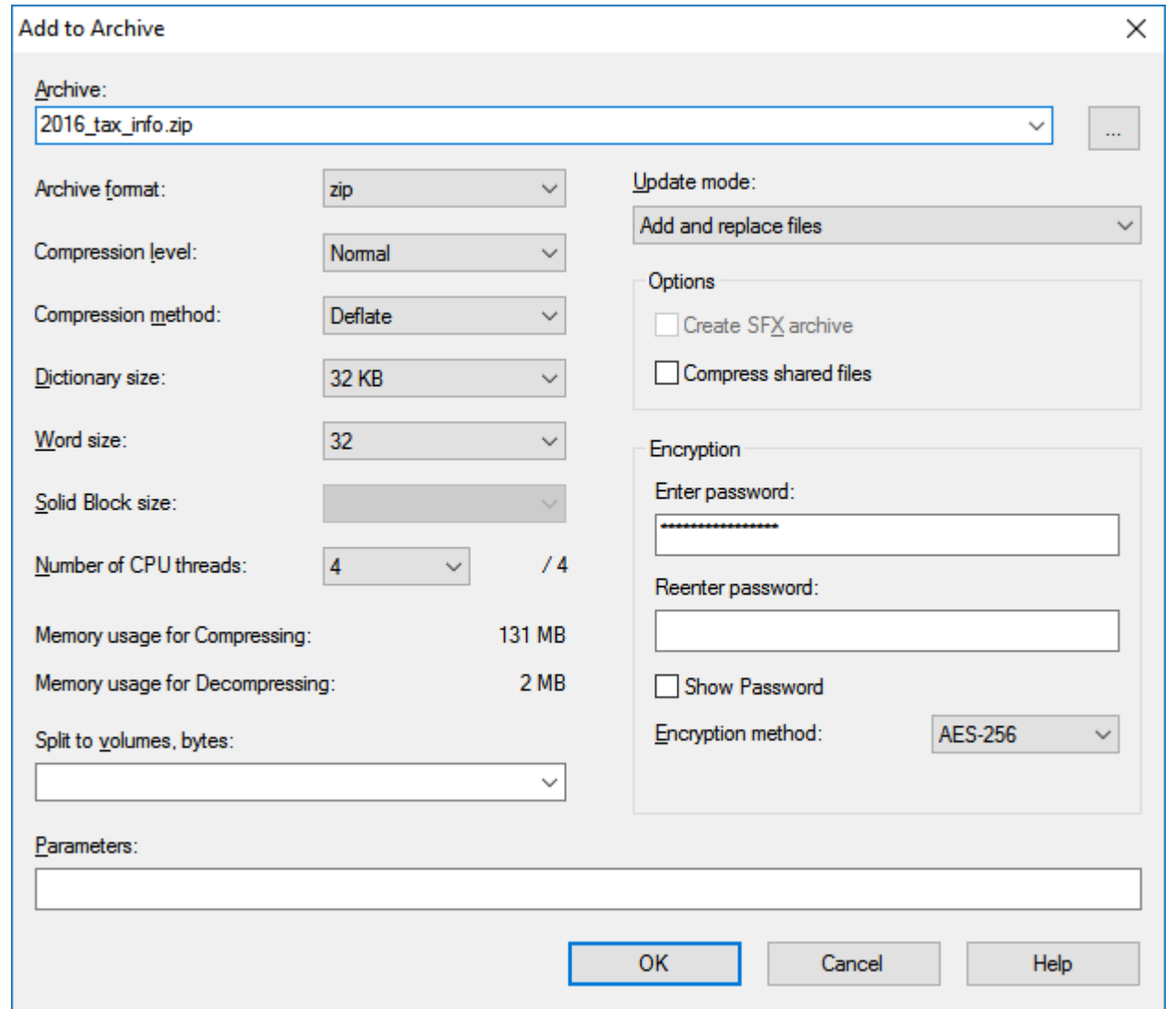


7-zip in use

Password needs to be sent to recipient by another method, e.g. phone or SMS.

The resulting .zip file is attached to an email.

Recipient needs 7-zip installed in order to decrypt the attachment.







Social Media

- Extreme caution is needed with personal information you provide on any website, but especially Social Media sites (*Facebook, Twitter, LinkedIn* etc.). Never provide your real Date of Birth or address.
- Privacy Settings need close attention since they often default to the most intrusive settings.
- Never provide your *Contacts List* to these sites. It is not your information to give out (under Privacy law) and you could infringe your friends' privacy.
- Read the site *Privacy Policy* before subscribing, e.g. [Facebook Privacy](#)

What is wrong with this?

Step 1
Find your friends

Are your friends already on Facebook?
Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook. See how it works.

 Outlook.com (Hotmail)	Find Friends
 Yahoo!	Find Friends
 Windows Live Messenger	Find Friends
 Other email service	

Please enter a valid username and password

Your Email

Email password

Find Friends

Problems with Facebook's "Add Friends" screen

- The request would provide Facebook with your email password, allowing them to access your Contacts list (and your email).
- Your Contacts list may contain private personal information about your friends, e.g. birthdays, home addresses, phone numbers. A fundamental privacy principle is that such information should never be released to other parties without permission.

Recommendation: Do not provide this information when setting up a new Facebook account, or any other Social Media account.

Facebook shares your information with other sites

In addition to the services offered by Facebook Inc. and Facebook Ireland Ltd, Facebook owns and operates each of the companies listed below, in accordance with their respective terms of service and privacy policies. We may share information about you within our family of companies to facilitate, support and integrate their activities and improve our services. For more information on the Facebook Companies' privacy practices and how they treat individuals' information, please visit the following links:

- Facebook Payments Inc. (https://www.facebook.com/payments_terms/privacy)
- Atlas (<http://atlassolutions.com/privacy-policy>)
- Instagram LLC (<http://instagram.com/about/legal/privacy/>)
- Onavo (http://www.onavo.com/privacy_policy)
- Parse (<https://parse.com/about/privacy>)
- Moves (<http://moves-app.com/privacy>)
- Oculus (<http://www.oculus.com/privacy/>)
- LiveRail (<http://www.liverail.com/privacy-policy/>)
- WhatsApp Inc. (<http://www.whatsapp.com/legal/#Privacy>)
- Masquerade (<https://www.facebook.com/msqrd/privacy>)

A Final Word

