# Sun City Computer Club

Cyber Security SIG

February 18, 2021

**Questions, Comments, Suggestions welcomed at any time**

**Even Now**

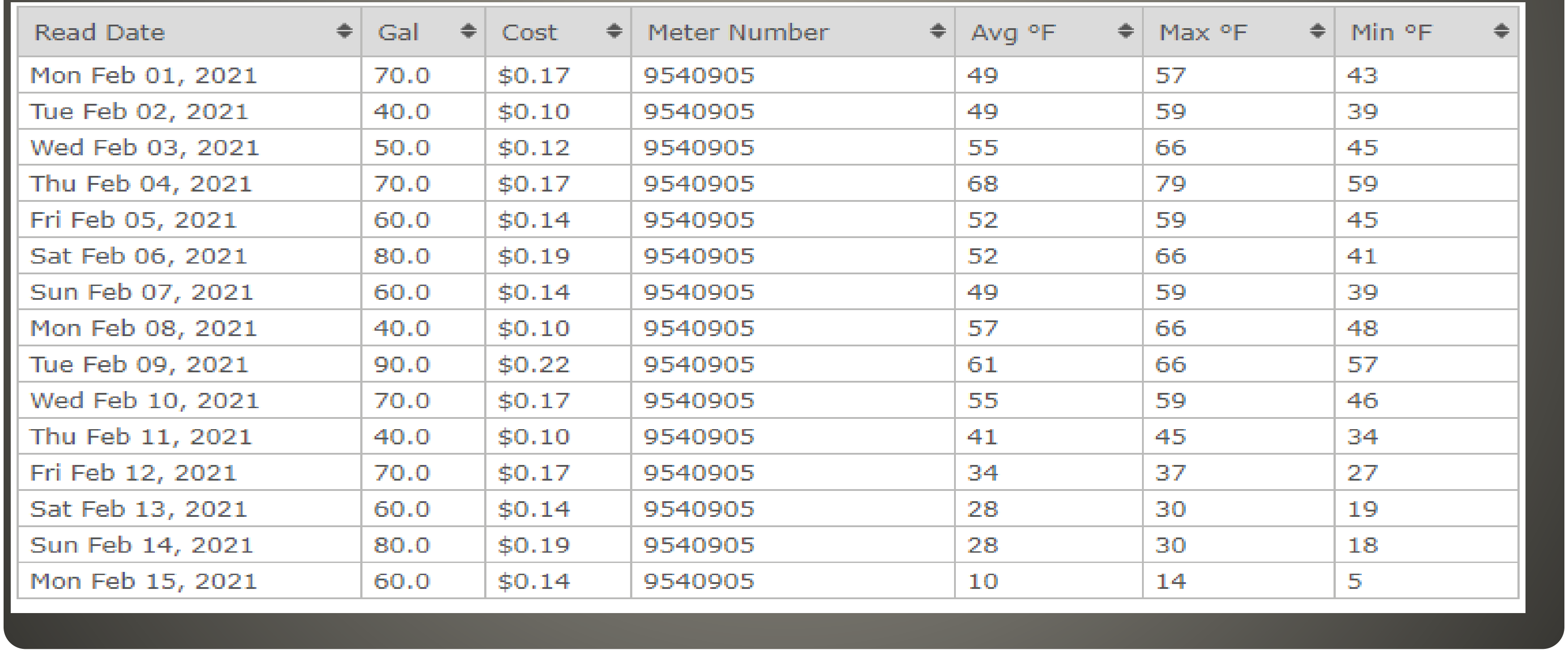
- Audio recording of this session as MP4 file
- Audio recording available at link shown above

**Audio Recording In Progress**

**SIG attendees are required to be members of the chartered club sponsoring that SIG.**
**Sun City Community Association By-law**

# Who knew?

- Georgetown Utility
- Account detail  water and electric
- https://guard.georgetown.org/index.php



| Read Date | Gal | Cost | Meter Number | Avg °F | Max °F | Min °F |
|---|---|---|---|---|---|---|
| Mon Feb 01, 2021 | 70.0 | $0.17 | 9540905 | 49 | 57 | 43 |
| Tue Feb 02, 2021 | 40.0 | $0.10 | 9540905 | 49 | 59 | 39 |
| Wed Feb 03, 2021 | 50.0 | $0.12 | 9540905 | 55 | 66 | 45 |
| Thu Feb 04, 2021 | 70.0 | $0.17 | 9540905 | 68 | 79 | 59 |
| Fri Feb 05, 2021 | 60.0 | $0.14 | 9540905 | 52 | 59 | 45 |
| Sat Feb 06, 2021 | 80.0 | $0.19 | 9540905 | 52 | 66 | 41 |
| Sun Feb 07, 2021 | 60.0 | $0.14 | 9540905 | 49 | 59 | 39 |
| Mon Feb 08, 2021 | 40.0 | $0.10 | 9540905 | 57 | 66 | 48 |
| Tue Feb 09, 2021 | 90.0 | $0.22 | 9540905 | 61 | 66 | 57 |
| Wed Feb 10, 2021 | 70.0 | $0.17 | 9540905 | 55 | 59 | 46 |
| Thu Feb 11, 2021 | 40.0 | $0.10 | 9540905 | 41 | 45 | 34 |
| Fri Feb 12, 2021 | 70.0 | $0.17 | 9540905 | 34 | 37 | 27 |
| Sat Feb 13, 2021 | 60.0 | $0.14 | 9540905 | 28 | 30 | 19 |
| Sun Feb 14, 2021 | 80.0 | $0.19 | 9540905 | 28 | 30 | 18 |
| Mon Feb 15, 2021 | 60.0 | $0.14 | 9540905 | 10 | 14 | 5 |

# Cellular Tether

- Laptop with charged battery
- USB cable cell phone    cellular data
- Use for power outage
- Use for Suddenlink outage
- Use for enhanced security

# Current Issues

- BigSur sudo
  Release version 1.9.5p2
  Beta version 1.8.31
- Google & Chrome sync
- Microsoft & Chrome as malware
- Zoom updates PER USER
- iOS “Safe Browsing” through Apple
- Super Micro – China
- SIM-Swapping
- Increased WEB Shell usage
- Apple M1 malware target

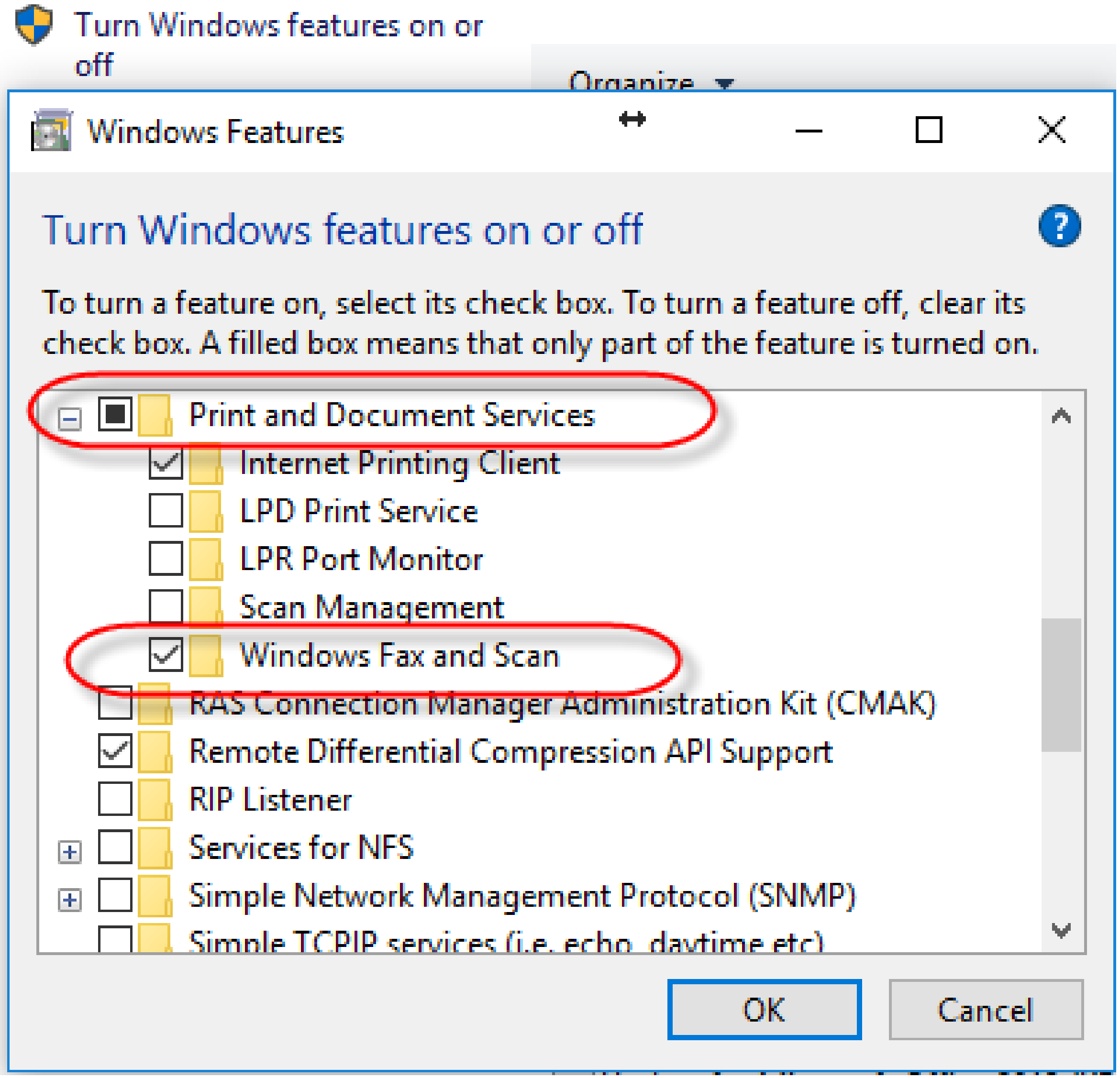
- eMail tracker pixels
- Medical devices  iPhone 12  MagSafe
- Adobe PDF tools Acrobat & Reader
- Microsoft patch Tuesday

  low number, high criticality   fax

  IPv4 source routing  CVSS 9.8

  IPv6 packet reassembly  CVSS 9.8
- Android SHAREit  transfer and share app
- Zoom updates are per user
- Copyrighted music to avoid live streaming

# Current Issues



## Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ⊟ ■ Print and Document Services
  - ☑ Internet Printing Client
  - □ LPD Print Service
  - □ LPR Port Monitor
  - □ Scan Management
  - ☑ Windows Fax and Scan
- □ RAS Connection Manager Administration Kit (CMAK)
- ☑ Remote Differential Compression API Support
- □ RIP Listener
- ⊞ □ Services for NFS
- ⊞ □ Simple Network Management Protocol (SNMP)
- □ Simple TCPIP services (i.e. echo, daytime etc)

# SCADA

- Oldsmar, Florida
- Sodium Hydroxide – lye
- 11,000% above “normal”
- RDP
- Remoteutilities.com
- Supervisory Control and Data Acquisition
- Windows 7
- Shared passphrase, no MFA, no firewall,
- Why/how did we learn? How many others?
- COMB ?
- If so …

# SCADA

- Florida county sheriff
- Intruder or insider (disgruntled)
- 54,000 district drinking water systems US
- Virtually ALL rely on remote access
- Virtually all are non segmented
- America’s Water Infrastructure Act 2018 *more than 3300 develop or update risk assessments and emergency response plans*
- Island hopping or add to bot net
- TeamViewer bad, but not worst no protection

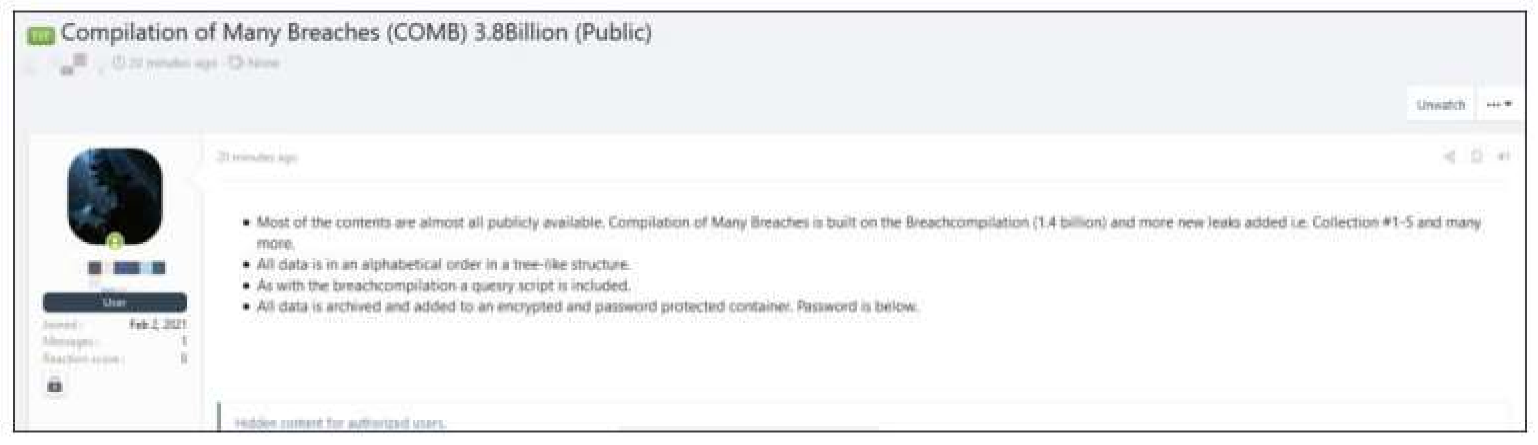
# SCADA

- Who checks risk assessments?
- Who checks response plans?
- Paper only??
- This time – alter treatment
- Next time – alter water quality safety
- Social media “boil notice”

- Social Media “poison notice”

# Current Issues

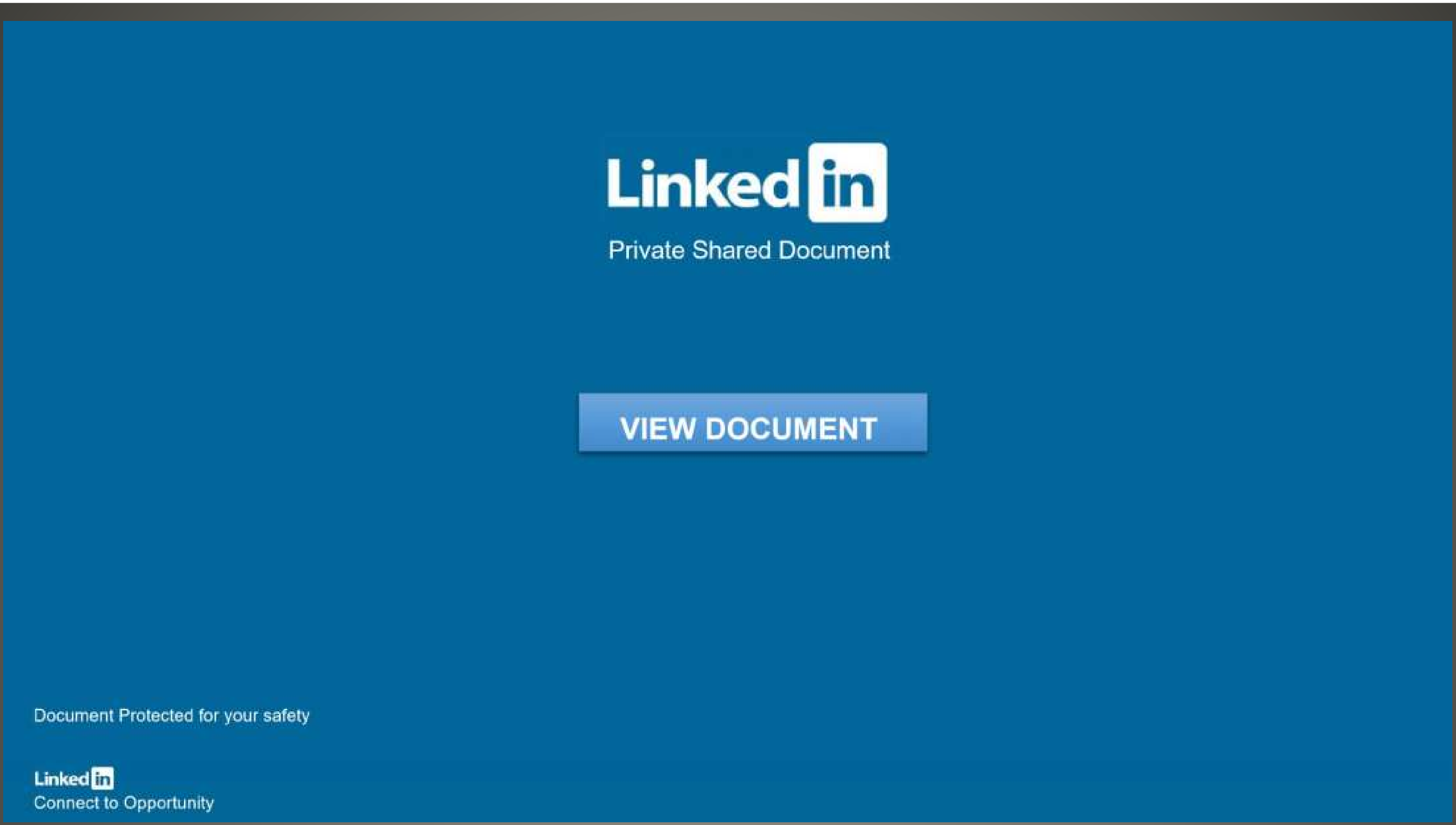
- WEB Shells 77,000 -> 140,000
  planted on web servers
  Planted in vulnerability “window”
  Hidden in *plain* sight/site
- WordPress
- COMB



Compilation of Many Breaches (COMB) 3.8Billion (Public)

- Most of the contents are almost all publicly available. Compilation of Many Breaches is built on the Breachcompilation (1.4 billion) and more new leaks added i.e. Collection #1-5 and many more.
- All data is in an alphabetical order in a tree-like structure.
- As with the breachcompilation a query script is included.
- All data is archived and added to an encrypted and password protected container. Password is below.

Hidden content for authorized users.



Linked in

Private Shared Document

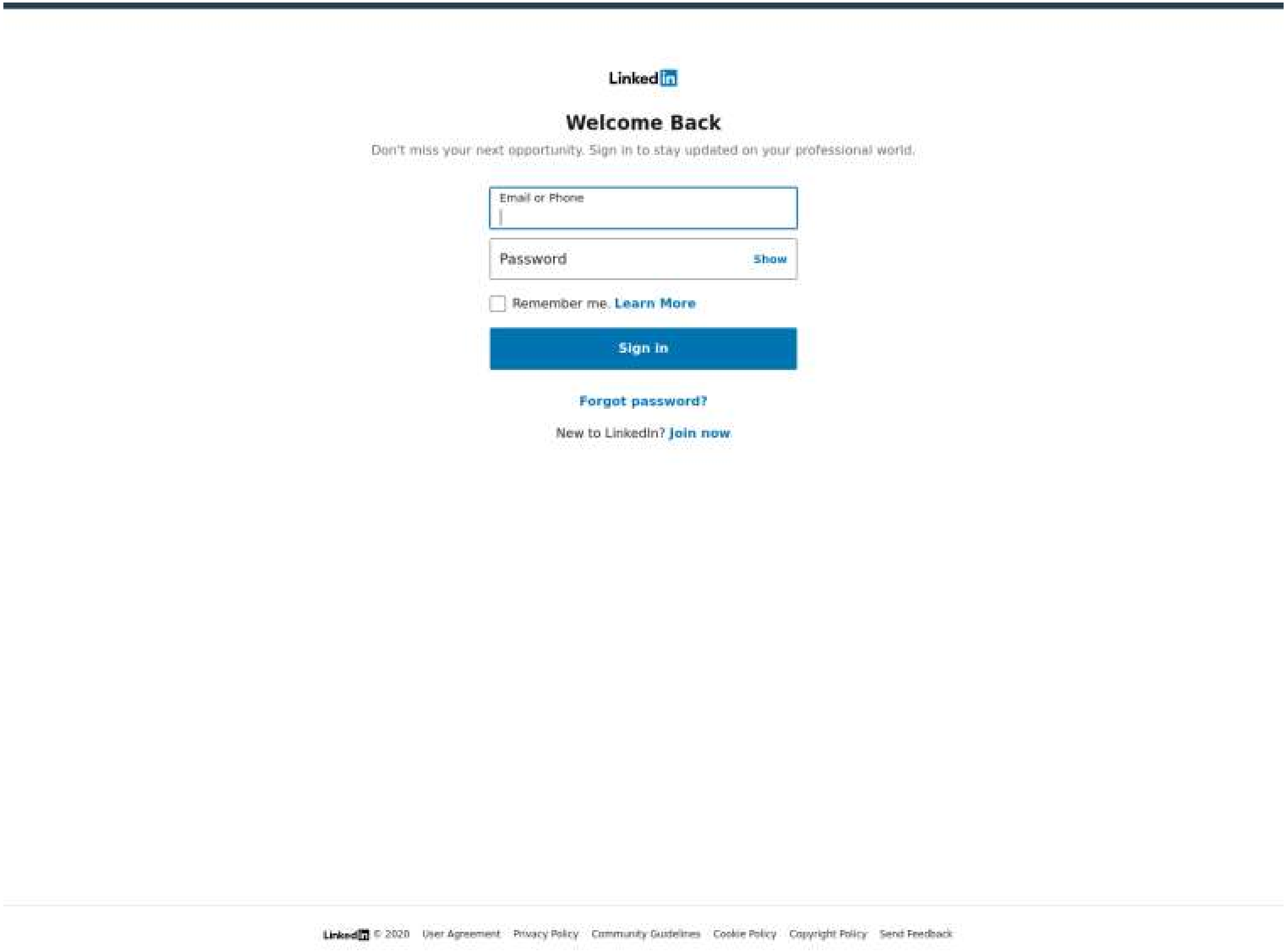
VIEW DOCUMENT

Document Protected for your safety

Linked in

Connect to Opportunity

# LinkedIn new feature? Not

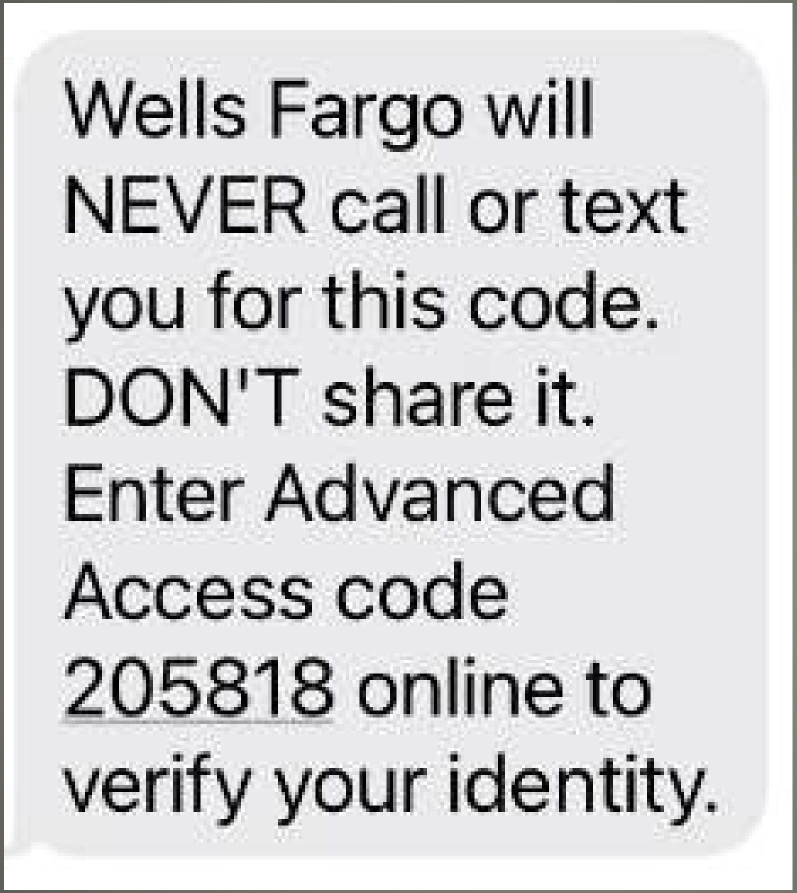


Welcome Back

Don't miss your next opportunity. Sign in to stay updated on your professional world.

- Notify any/everyone you receive from
- Consider changing passcode  add MFA
- COMB

# LinkedIn



Wells Fargo will NEVER call or text you for this code. DON'T share it. Enter Advanced Access code 205818 online to verify your identity.

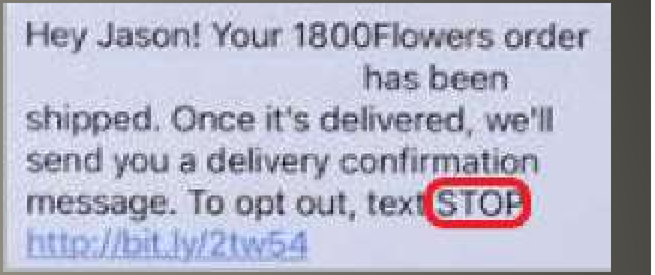
# Current Issues

# COMB

- Compilation
- Clear text passwords/passphrases
- 200 million Gmail   450 million yahoo
- Fast lookup, FASTER credential stuffing
- Long unused accounts taken over
- If taken over …
- CHANGE passphrases
- ADD MFA
- KEEP inventory

# SPAM Text, Voice Mail?

- Smart Phones
- DO NOT click – Open links
- Maby STOP
- Maby not
- Forward "SPAM" 7726



Hey Jason! Your 1800Flowers order has been shipped. Once it's delivered, we'll send you a delivery confirmation message. To opt out, text STOP http://bit.ly/2tw54

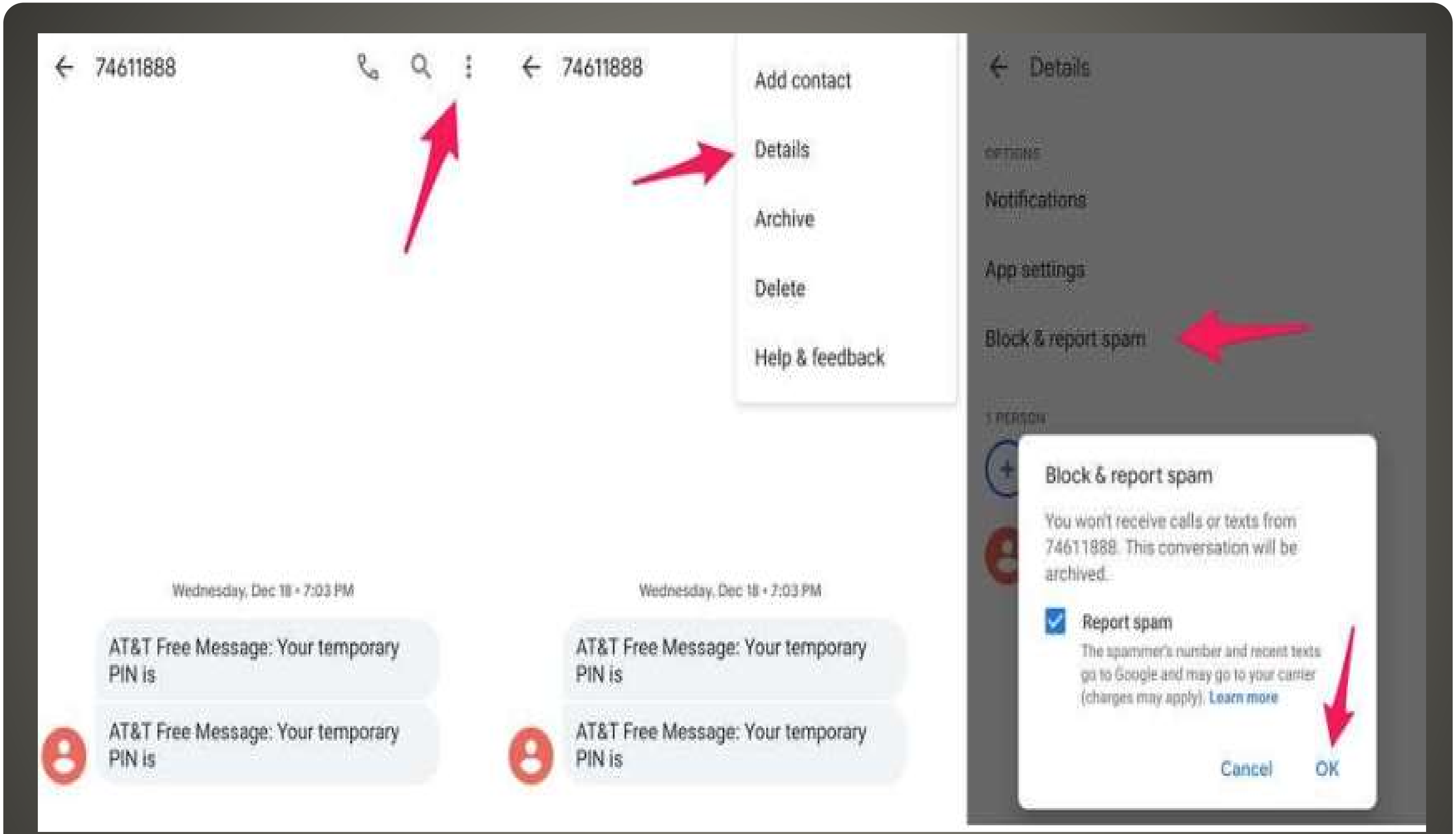
- https://consumercomplaints.fcc.gov/hc/en-us

# SPAM avoidance

- Multiple email providers/addresses
- Name at dot domain
- Donald[at]Disney[.]com
- Privacy policy
- “get notices?”
- Breach subject?
- Australia

# Robocalls

- Land Line  Caller ID
- SHAKEN/STIR
- **S**ecure **H**andling of **A**sserted information using to**kens**
- **S**ecure **T**elephone **I**dentity **R**evisited
- Traced Act
- **T**elephone **R**obocall **A**buse **C**riminal **E**nforcement and **D**eterrence



Wednesday, Dec 18 • 7:03 PM

AT&T Free Message: Your temporary PIN is

AT&T Free Message: Your temporary PIN is

Wednesday, Dec 18 • 7:03 PM

AT&T Free Message: Your temporary PIN is

AT&T Free Message: Your temporary PIN is

Block & report spam

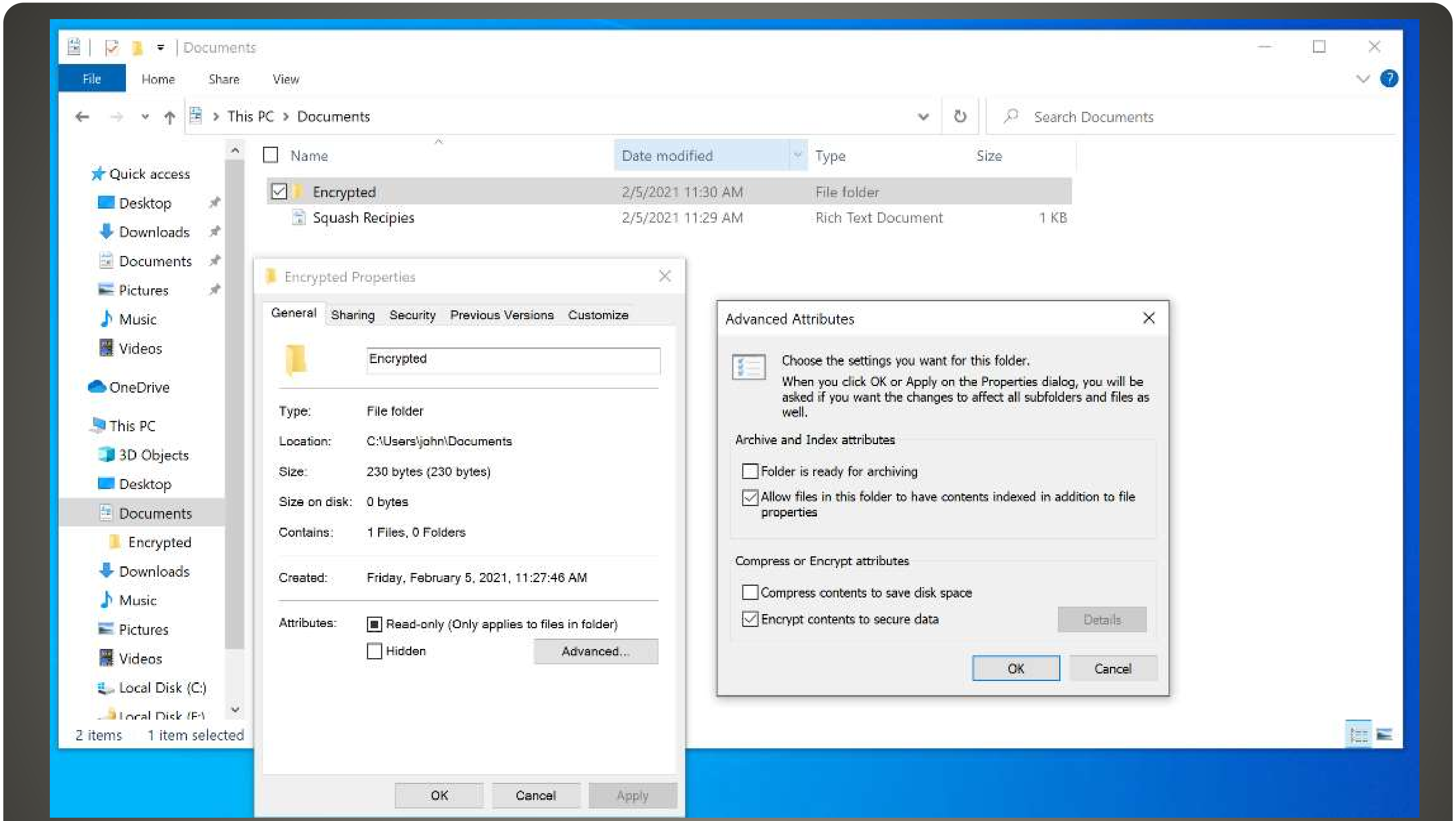
You won't receive calls or texts from 74611888. This conversation will be archived.

☑ Report spam

The spammer's number and recent texts go to Google and may go to your carrier (charges may apply). Learn more

# Encryption for Protection

- DOUBLE EDGED SWORD
- Cloud
- Digital Will



| Name | Date modified | Type | Size |
|---|---|---|---|
| ☑ Encrypted | 2/5/2021 11:30 AM | File folder | |
| Squash Recipies | 2/5/2021 11:29 AM | Rich Text Document | 1 KB |

Encrypted

Type: File folder

Location: C:\Users\john\Documents

Size: 230 bytes (230 bytes)

Size on disk: 0 bytes

Contains: 1 Files, 0 Folders

Created: Friday, February 5, 2021, 11:27:46 AM

Attributes: ■ Read-only (Only applies to files in folder)

□ Hidden

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

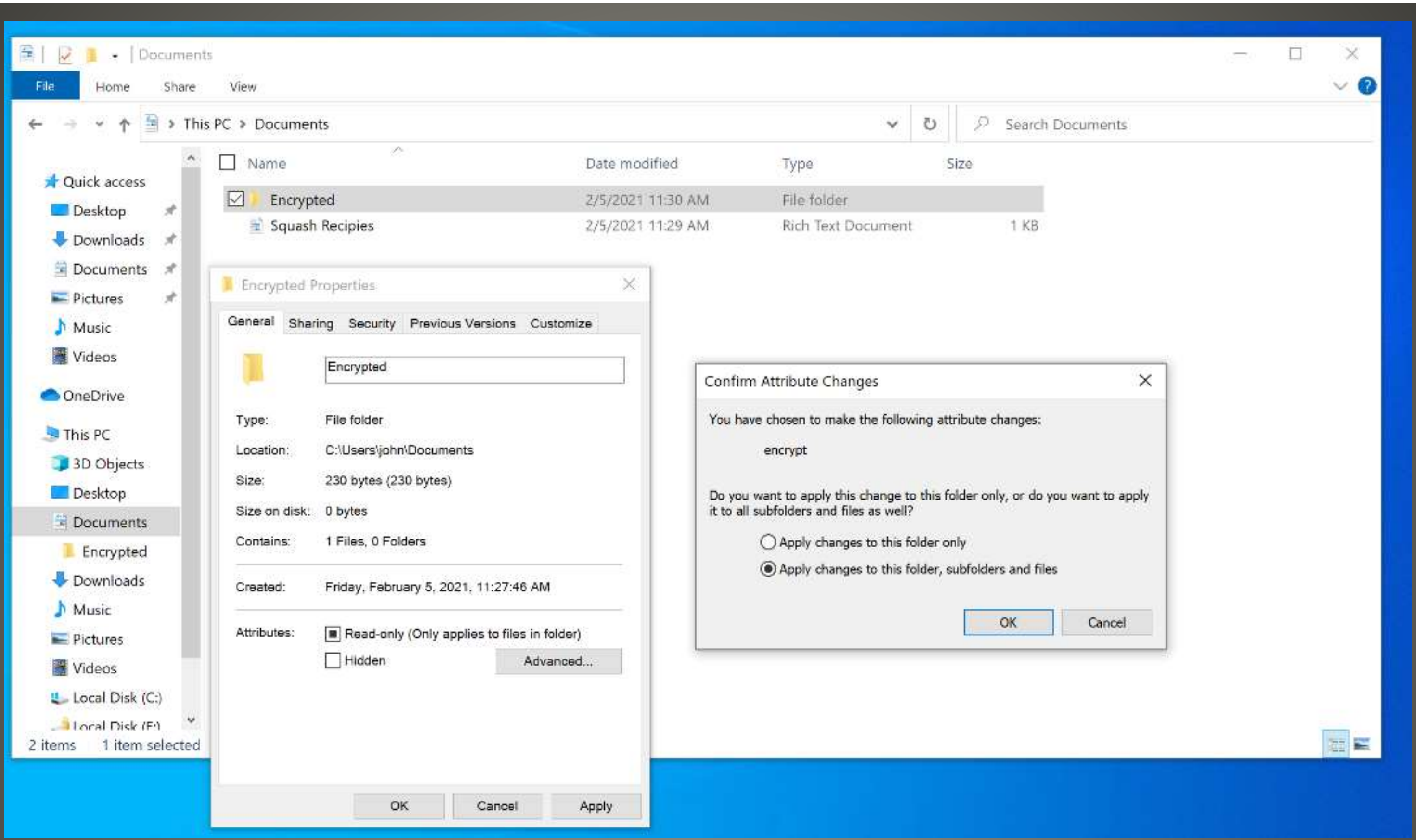
☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

# Windows PRO folder



| Name | Date modified | Type | Size |
|---|---|---|---|
| ☑ Encrypted | 2/5/2021 11:30 AM | File folder | |
| Squash Recipies | 2/5/2021 11:29 AM | Rich Text Document | 1 KB |

Encrypted Properties

Encrypted

Type: File folder

Location: C:\Users\john\Documents

Size: 230 bytes (230 bytes)

Size on disk: 0 bytes

Contains: 1 Files, 0 Folders

Created: Friday, February 5, 2021, 11:27:46 AM

Attributes: ■ Read-only (Only applies to files in folder)

□ Hidden

Confirm Attribute Changes

You have chosen to make the following attribute changes:

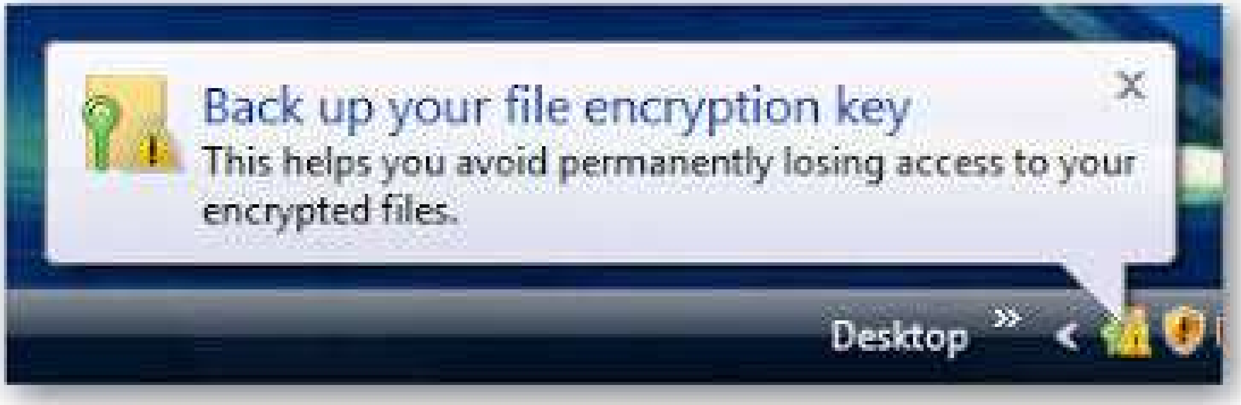
encrypt

Do you want to apply this change to this folder only, or do you want to apply it to all subfolders and files as well?

○ Apply changes to this folder only

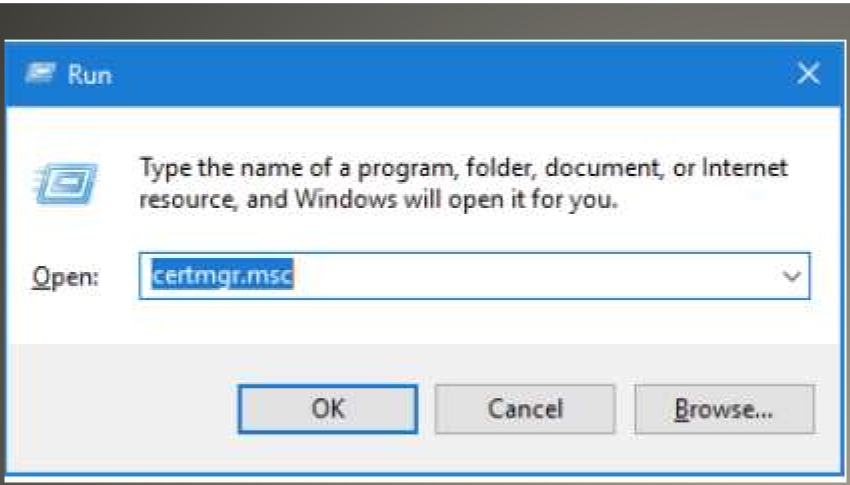
● Apply changes to this folder, subfolders and files

# Windows PRO folder Apply



Back up your file encryption key

This helps you avoid permanently losing access to your encrypted files.

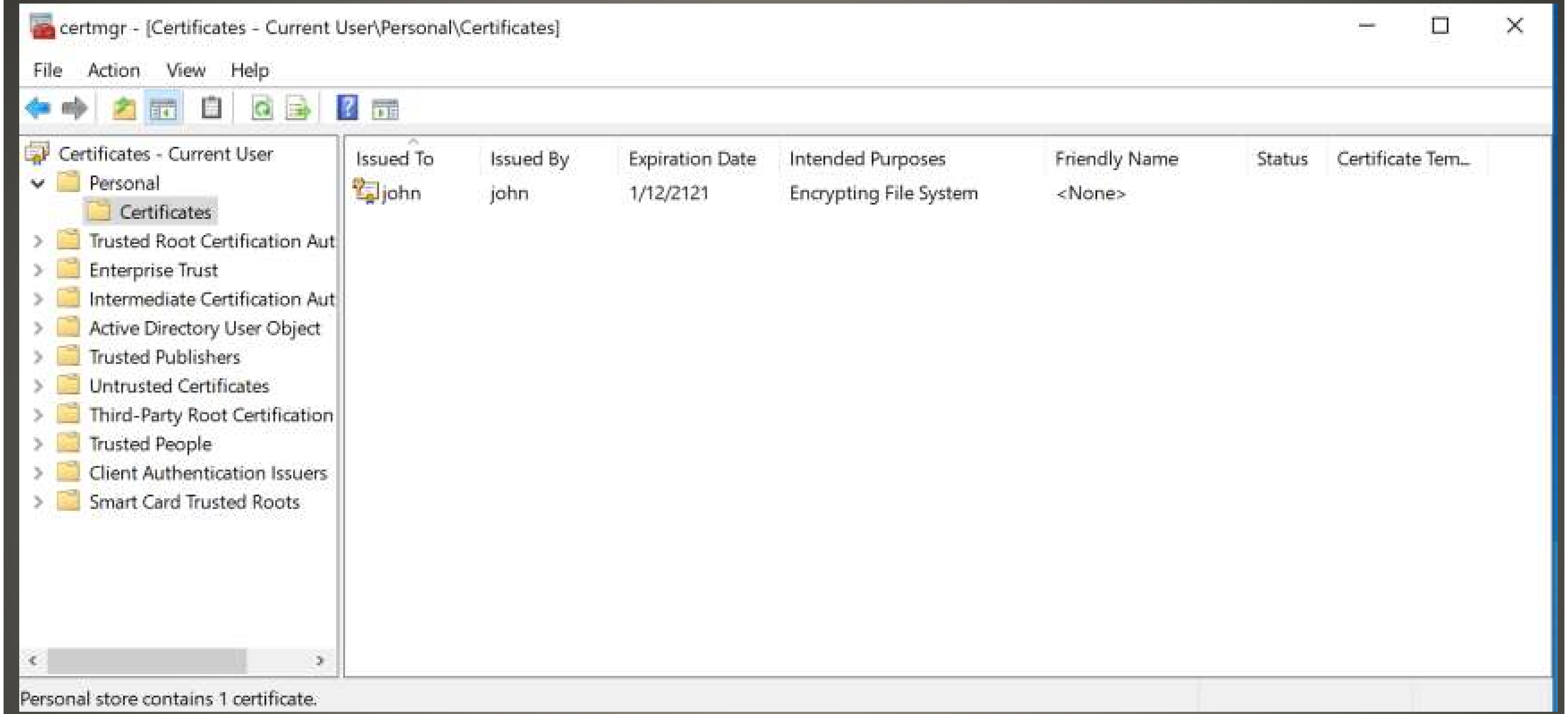


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: certmgr.msc

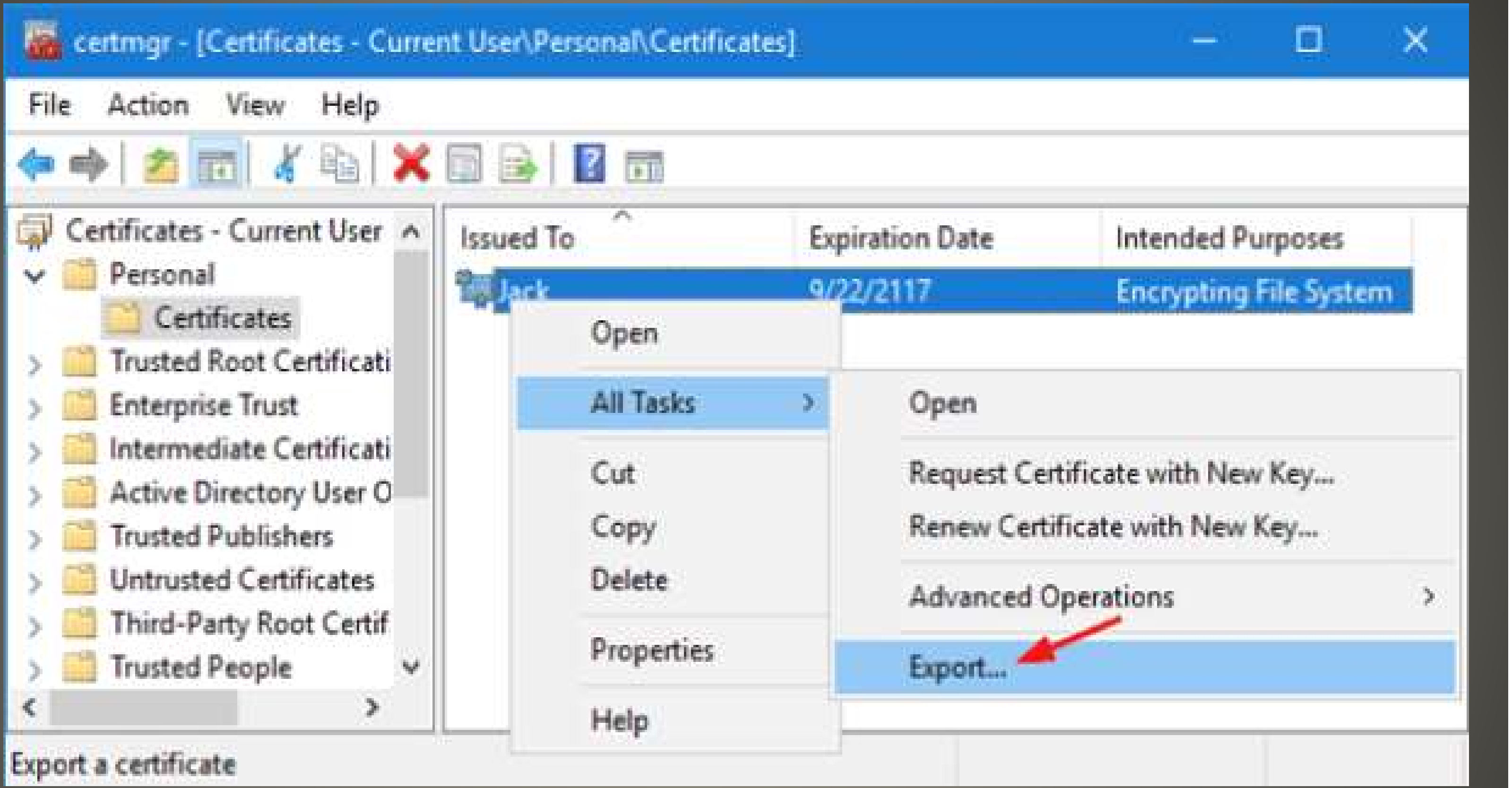
# EFS


certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Aut
Enterprise Trust
Intermediate Certification Aut
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Client Authentication Issuers
Smart Card Trusted Roots

| Issued To | Issued By | Expiration Date | Intended Purposes | Friendly Name | Status | Certificate Tem... |
|---|---|---|---|---|---|---|
| john | john | 1/12/2121 | Encrypting File System | <None> | | |

Personal store contains 1 certificate.

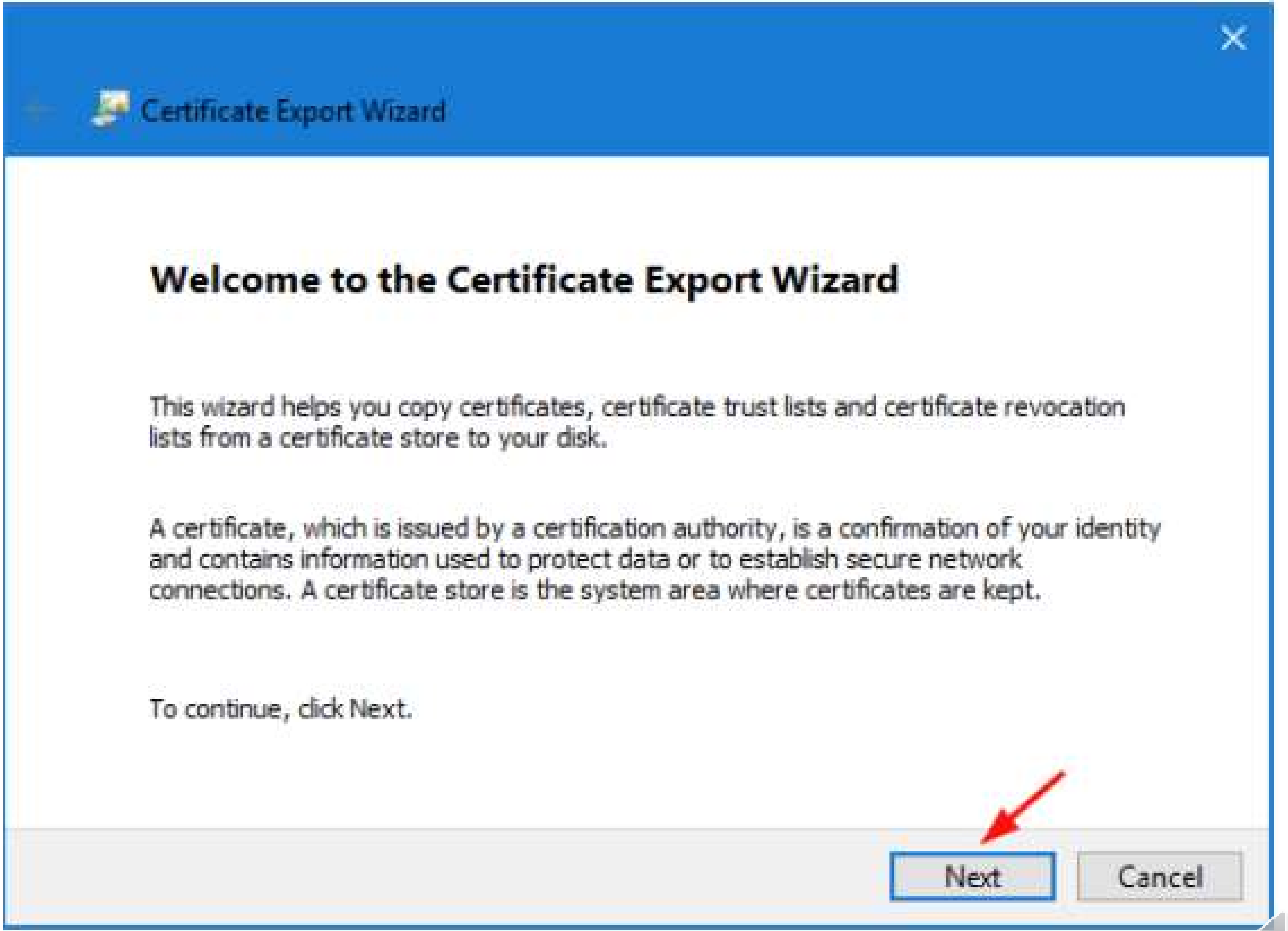
# EFS Certificate to backup/export



certmgr - [Certificates - Current User\Personal\Certificates]

| Issued To | Expiration Date | Intended Purposes |
|---|---|---|
| Jack | 9/22/2117 | Encrypting File System |

Export a certificate

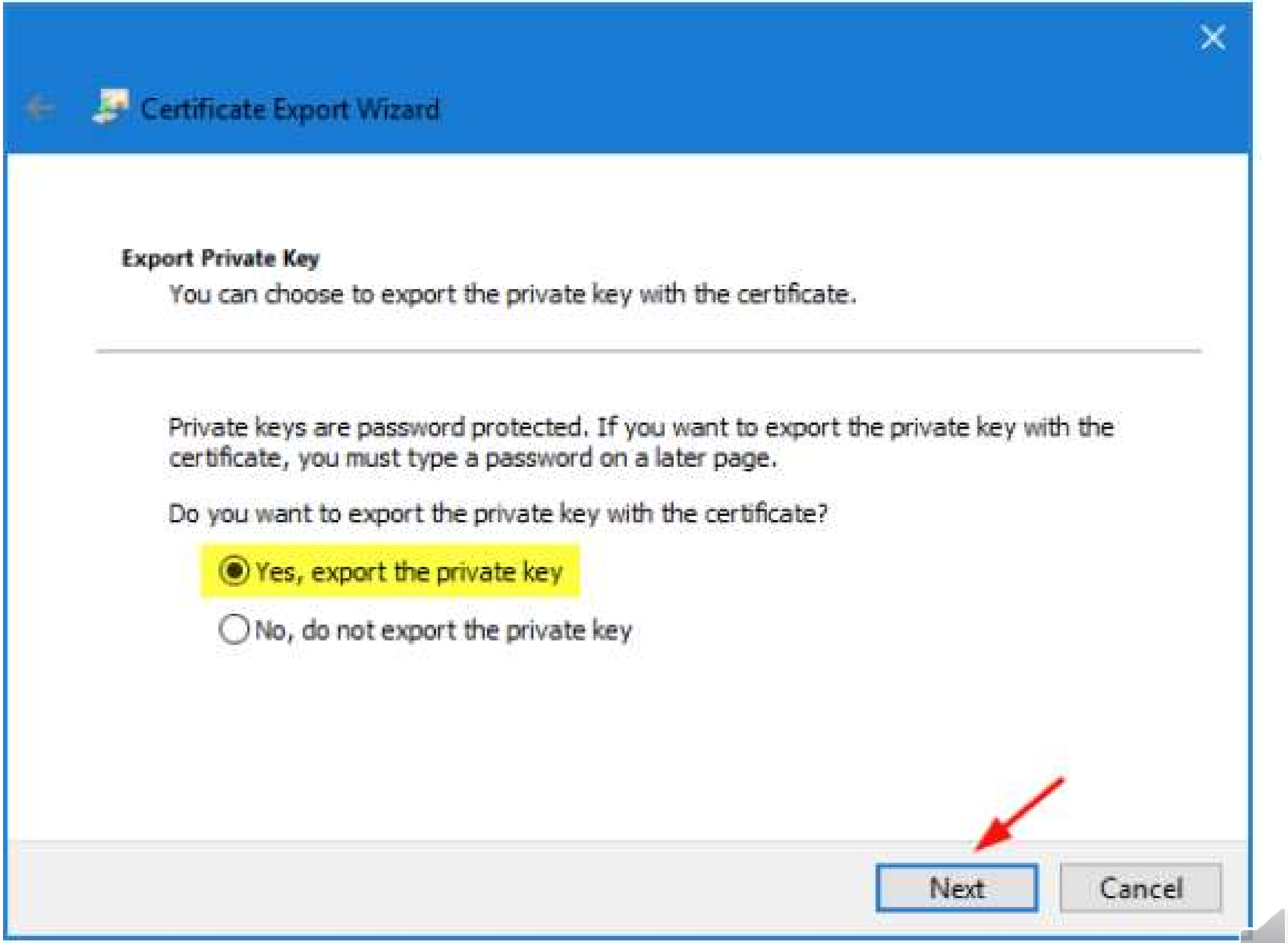


## Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.



Certificate Export Wizard

**Export Private Key**

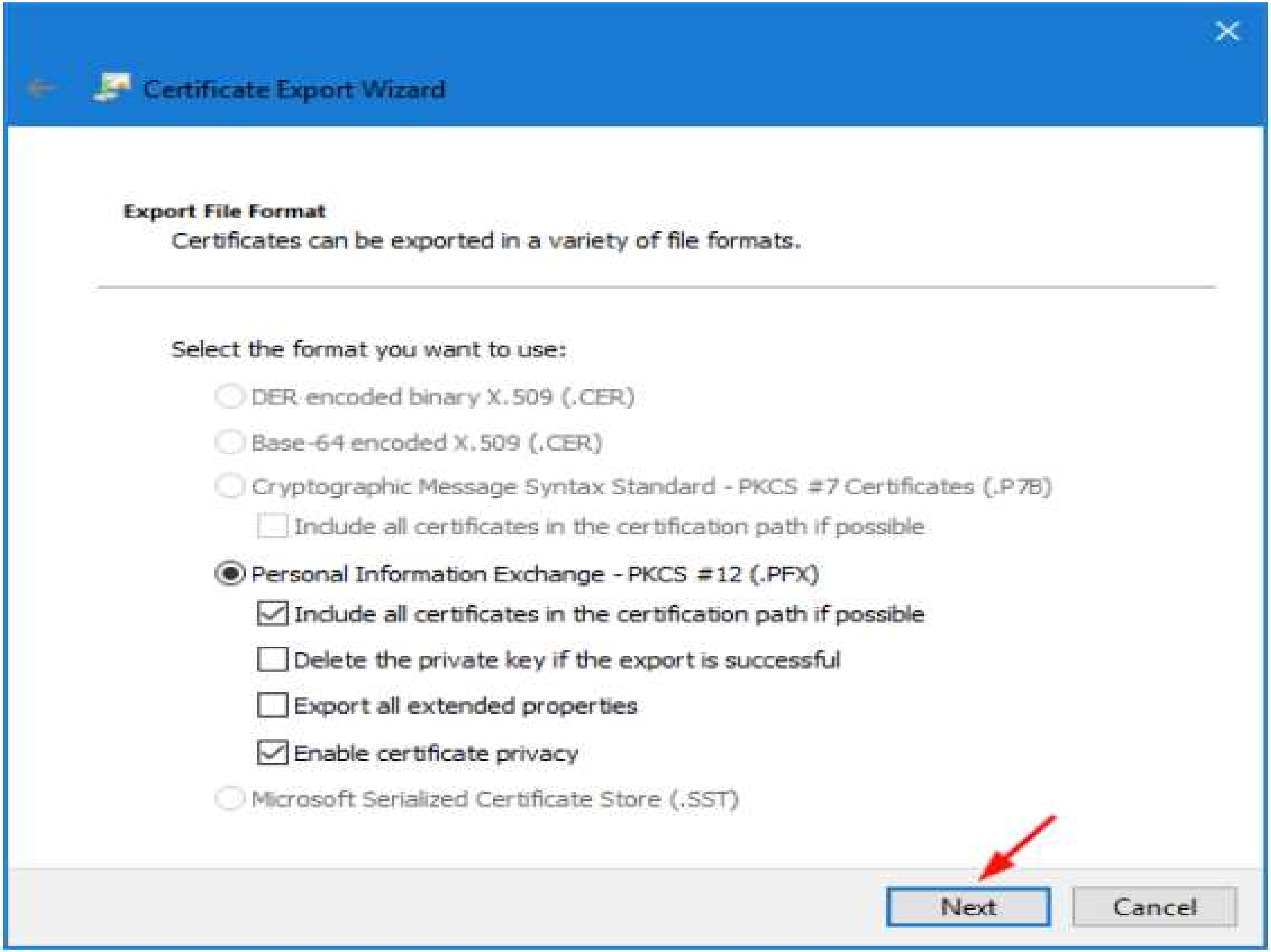
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key



**Export File Format**

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

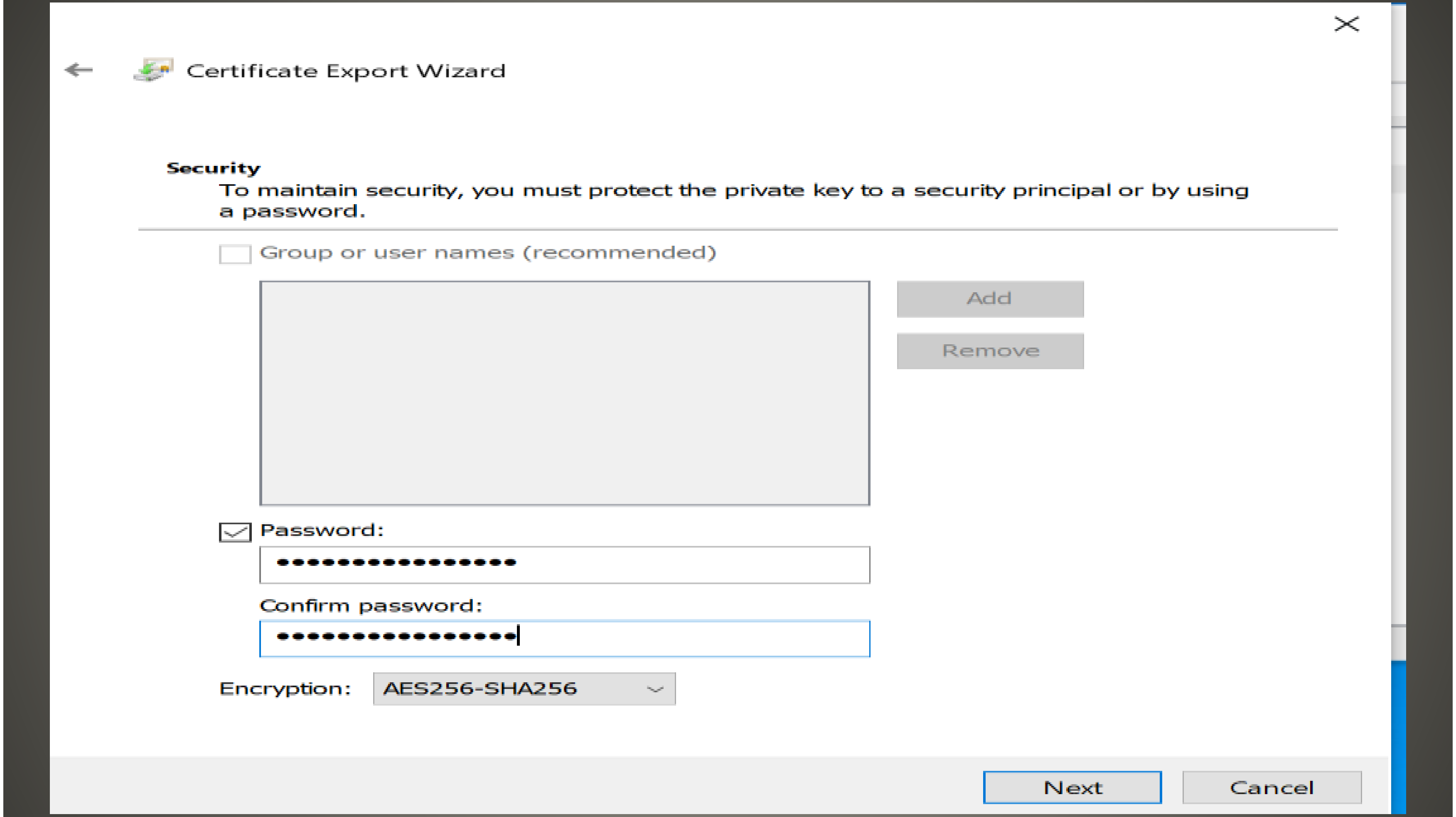
☑ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

☑ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)



Certificate Export Wizard

**Security**

To maintain security, you must protect the private key to a security principal or by using a password.

□ Group or user names (recommended)

☑ Password:

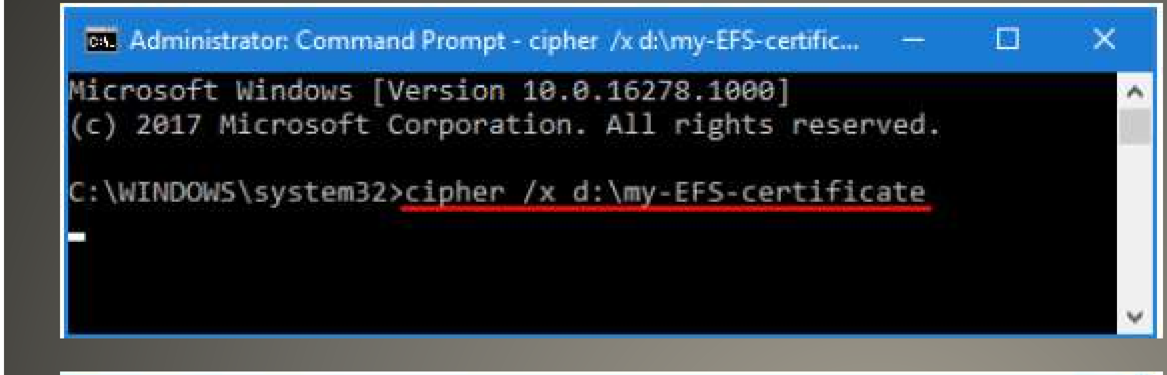
•••••••••••••••••

Confirm password:

•••••••••••••••••

Encryption: AES256-SHA256

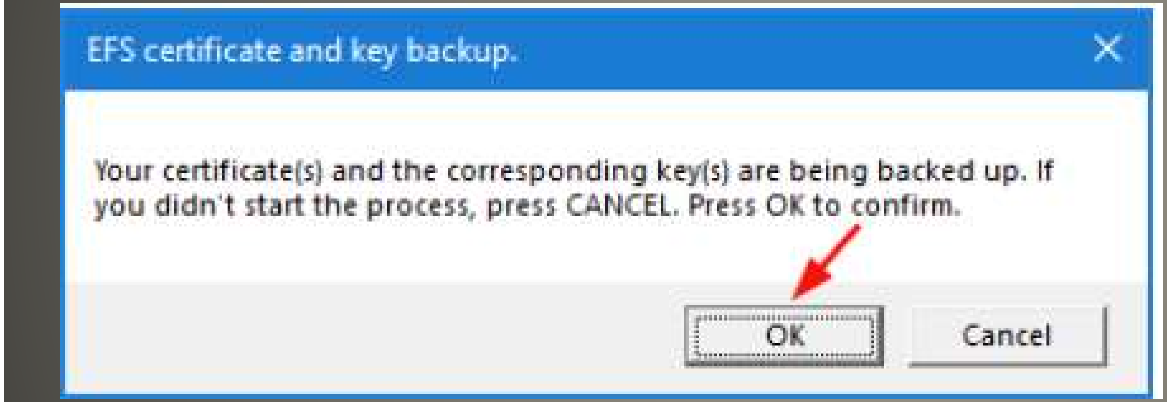
# Select location and Finish



Administrator: Command Prompt - cipher /x d:\my-EFS-certific...

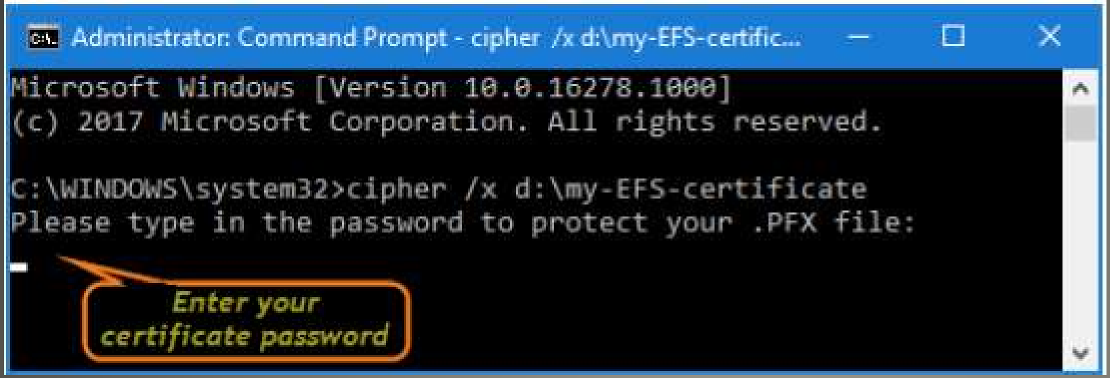
```
Microsoft Windows [Version 10.0.16278.1000]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cipher /x d:\my-EFS-certificate
```



Your certificate(s) and the corresponding key(s) are being backed up. If you didn't start the process, press CANCEL. Press OK to confirm.

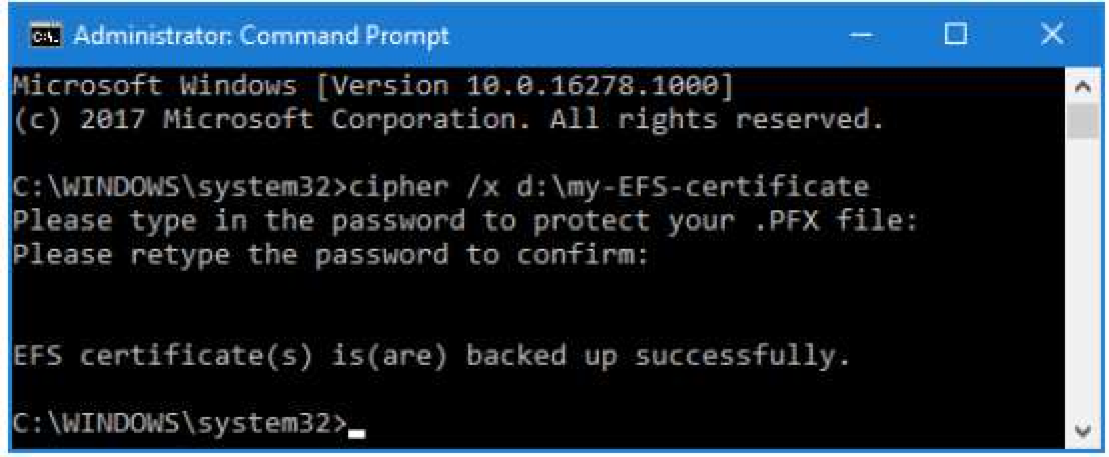
# Or use Commands


Administrator: Command Prompt - cipher /x d:\my-EFS-certific...

```
Microsoft Windows [Version 10.0.16278.1000]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cipher /x d:\my-EFS-certificate
Please type in the password to protect your .PFX file:
_
```

Enter your certificate password

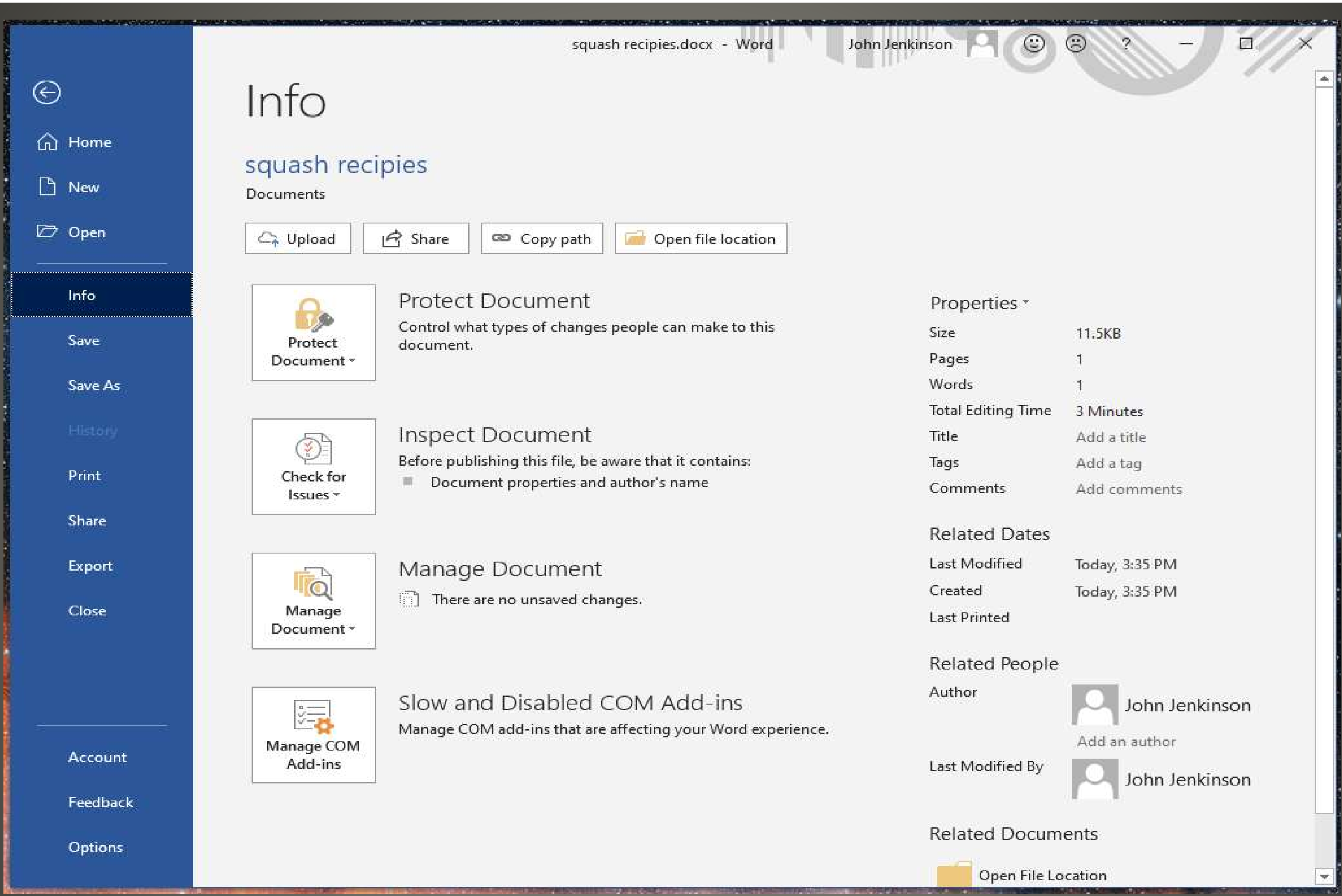


```
Microsoft Windows [Version 10.0.16278.1000]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cipher /x d:\my-EFS-certificate
Please type in the password to protect your .PFX file:
Please retype the password to confirm:


EFS certificate(s) is(are) backed up successfully.

C:\WINDOWS\system32>_
```



# Info

squash recipies

Documents

### Protect Document

Control what types of changes people can make to this document.

### Inspect Document

Before publishing this file, be aware that it contains:

- Document properties and author's name

### Manage Document

There are no unsaved changes.

### Slow and Disabled COM Add-ins

Manage COM add-ins that are affecting your Word experience.

Properties

| | |
|---|---|
| Size | 11.5KB |
| Pages | 1 |
| Words | 1 |
| Total Editing Time | 3 Minutes |
| Title | Add a title |
| Tags | Add a tag |
| Comments | Add comments |

Related Dates

| | |
|---|---|
| Last Modified | Today, 3:35 PM |
| Created | Today, 3:35 PM |
| Last Printed | |

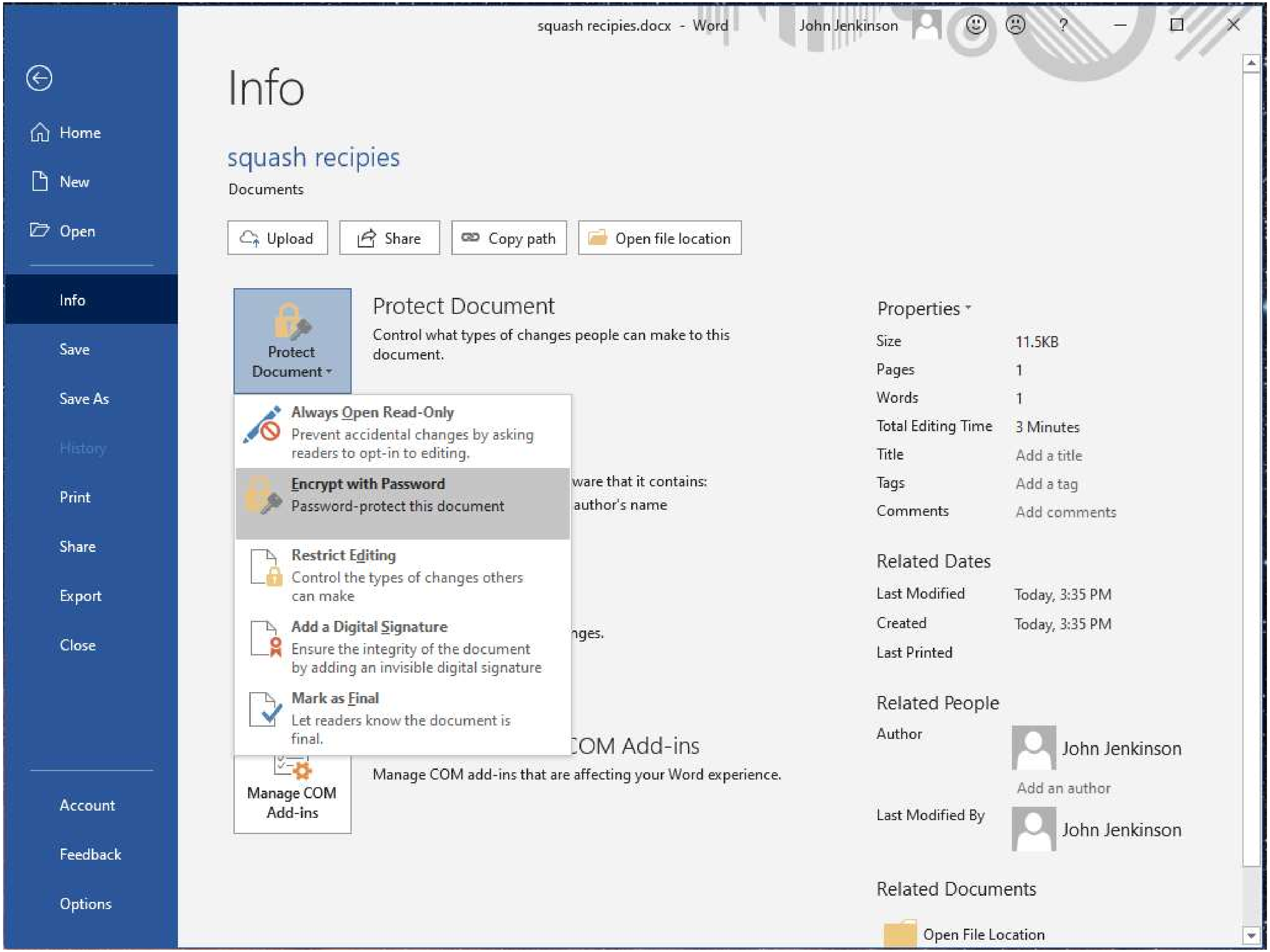
Related People

| | |
|---|---|
| Author | John Jenkinson<br>Add an author |
| Last Modified By | John Jenkinson |

Related Documents

Open File Location

# Office Document Password Protect



# Info

## squash recipies

Documents

### Protect Document

Control what types of changes people can make to this document.

**Always Open Read-Only**
Prevent accidental changes by asking readers to opt-in to editing.

**Encrypt with Password**
Password-protect this document

**Restrict Editing**
Control the types of changes others can make

**Add a Digital Signature**
Ensure the integrity of the document by adding an invisible digital signature

**Mark as Final**
Let readers know the document is final.

ware that it contains:

author's name

nges.

### COM Add-ins

Manage COM add-ins that are affecting your Word experience.

### Properties

| | |
|---|---|
| Size | 11.5KB |
| Pages | 1 |
| Words | 1 |
| Total Editing Time | 3 Minutes |
| Title | Add a title |
| Tags | Add a tag |
| Comments | Add comments |

### Related Dates

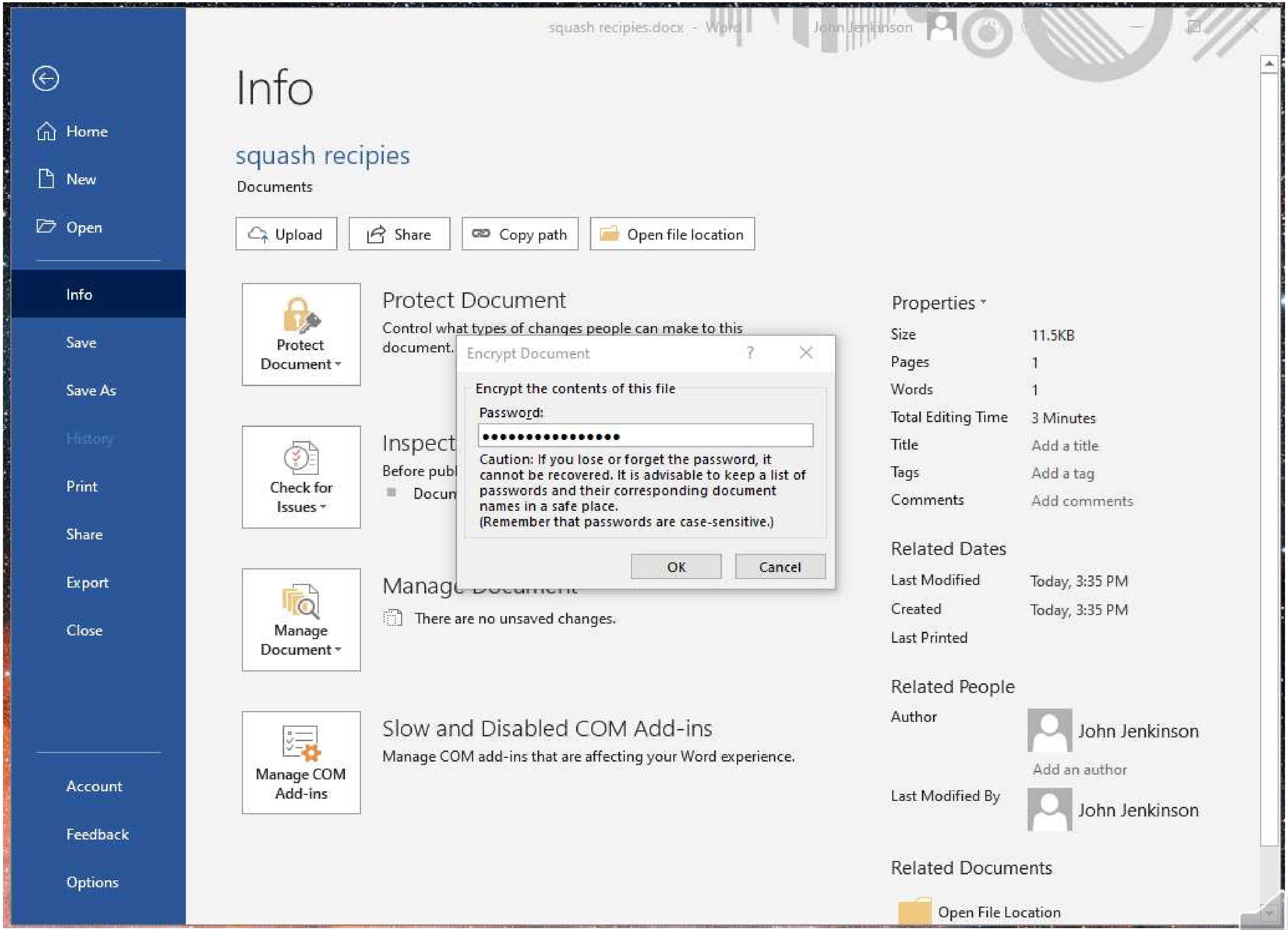
| | |
|---|---|
| Last Modified | Today, 3:35 PM |
| Created | Today, 3:35 PM |
| Last Printed | |

### Related People

| | |
|---|---|
| Author | John Jenkinson<br>Add an author |
| Last Modified By | John Jenkinson |

### Related Documents

Open File Location



# Info

squash recipies

Documents

## Protect Document

Control what types of changes people can make to this document.

## Inspect

Before publ

Docun

## Manage Document

There are no unsaved changes.

## Slow and Disabled COM Add-ins

Manage COM add-ins that are affecting your Word experience.

**Encrypt Document**

Encrypt the contents of this file

Password: ●●●●●●●●●●●●●●●●

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place.
(Remember that passwords are case-sensitive.)

Properties

| | |
|---|---|
| Size | 11.5KB |
| Pages | 1 |
| Words | 1 |
| Total Editing Time | 3 Minutes |
| Title | Add a title |
| Tags | Add a tag |
| Comments | Add comments |

Related Dates

| | |
|---|---|
| Last Modified | Today, 3:35 PM |
| Created | Today, 3:35 PM |
| Last Printed | |

Related People

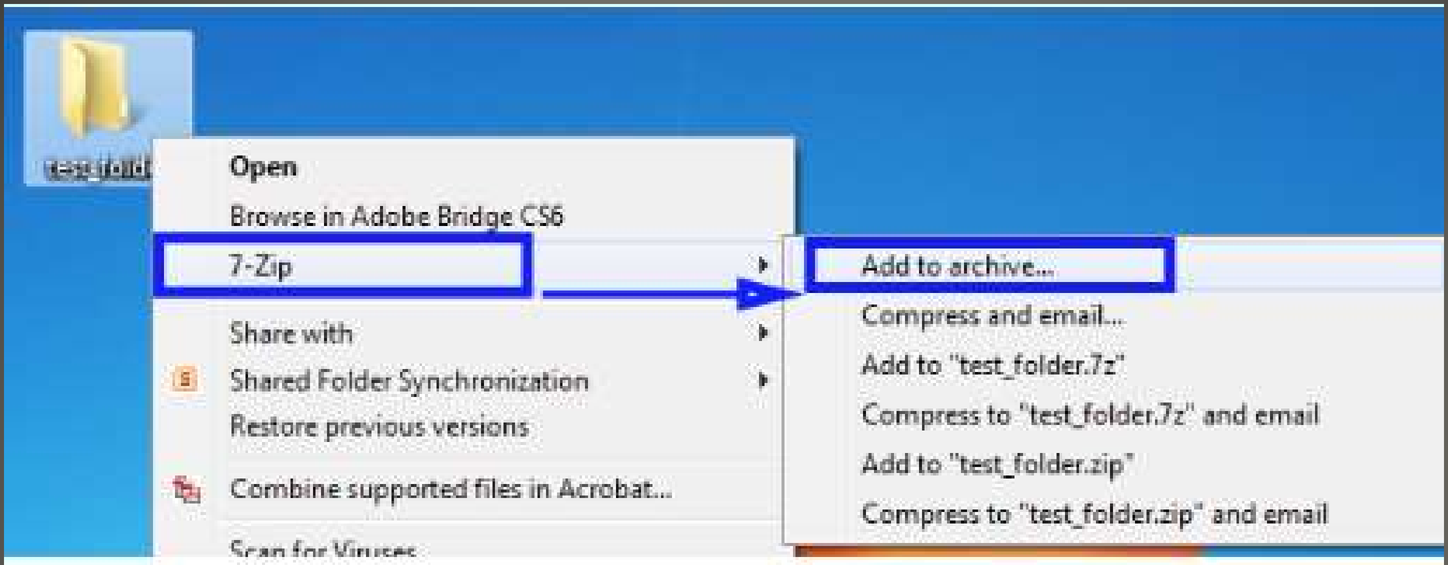
| | |
|---|---|
| Author | John Jenkinson<br>Add an author |
| Last Modified By | John Jenkinson |

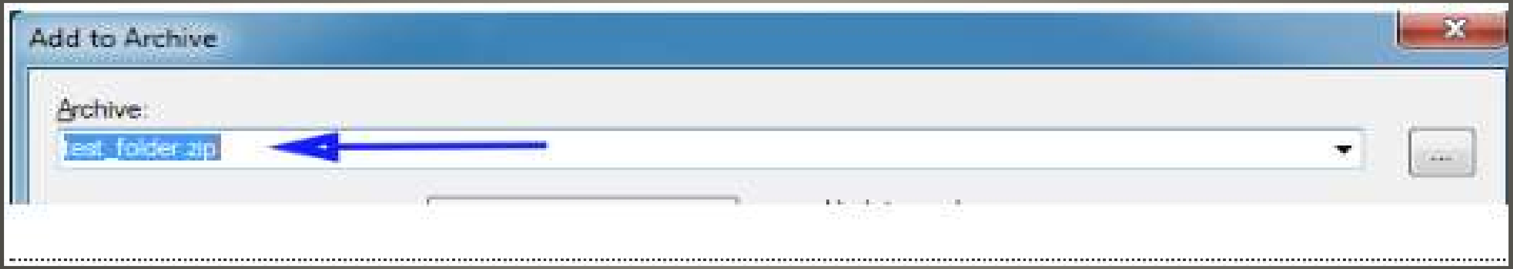
Related Documents

Open File Location

- No EFS
- Internet scripts
- WinRAR
- 7-Zip
- Microsoft Store

# Windows 10 Home

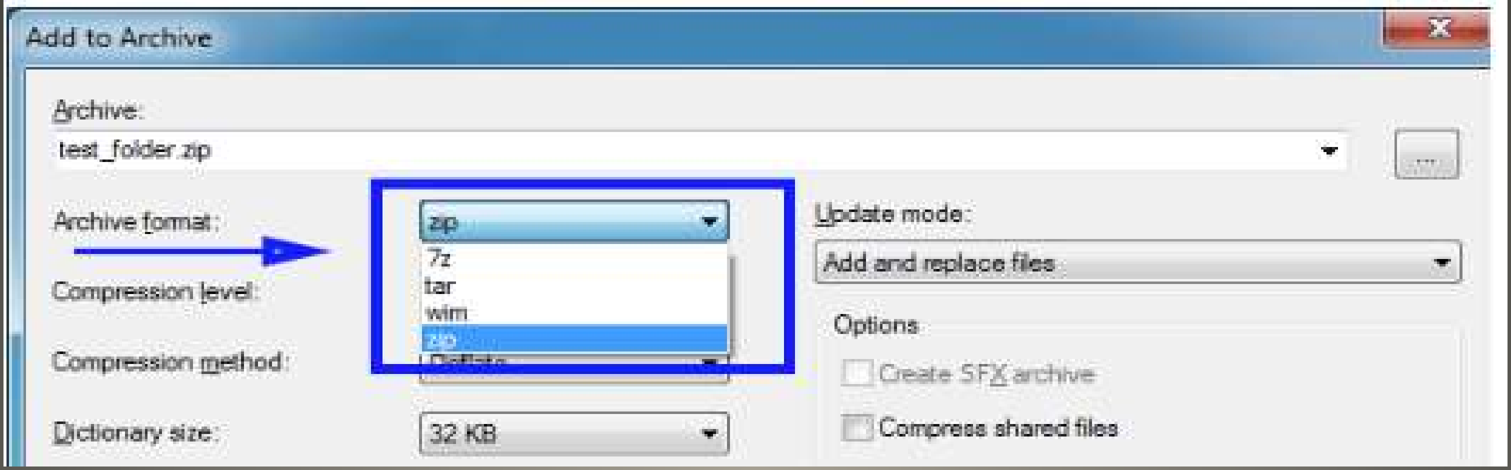

test_fold
Open
Browse in Adobe Bridge CS6
7-Zip
Share with
Shared Folder Synchronization
Restore previous versions
Combine supported files in Acrobat...
Scan for Viruses
Add to archive...
Compress and email...
Add to "test_folder.7z"
Compress to "test_folder.7z" and email
Add to "test_folder.zip"
Compress to "test_folder.zip" and email



Archive: test_folder.zip

# 7-Zip

# 7-Zip



Add to Archive

Archive: test_folder.zip

Archive format: zip

Compression level:

Compression method: Deflate

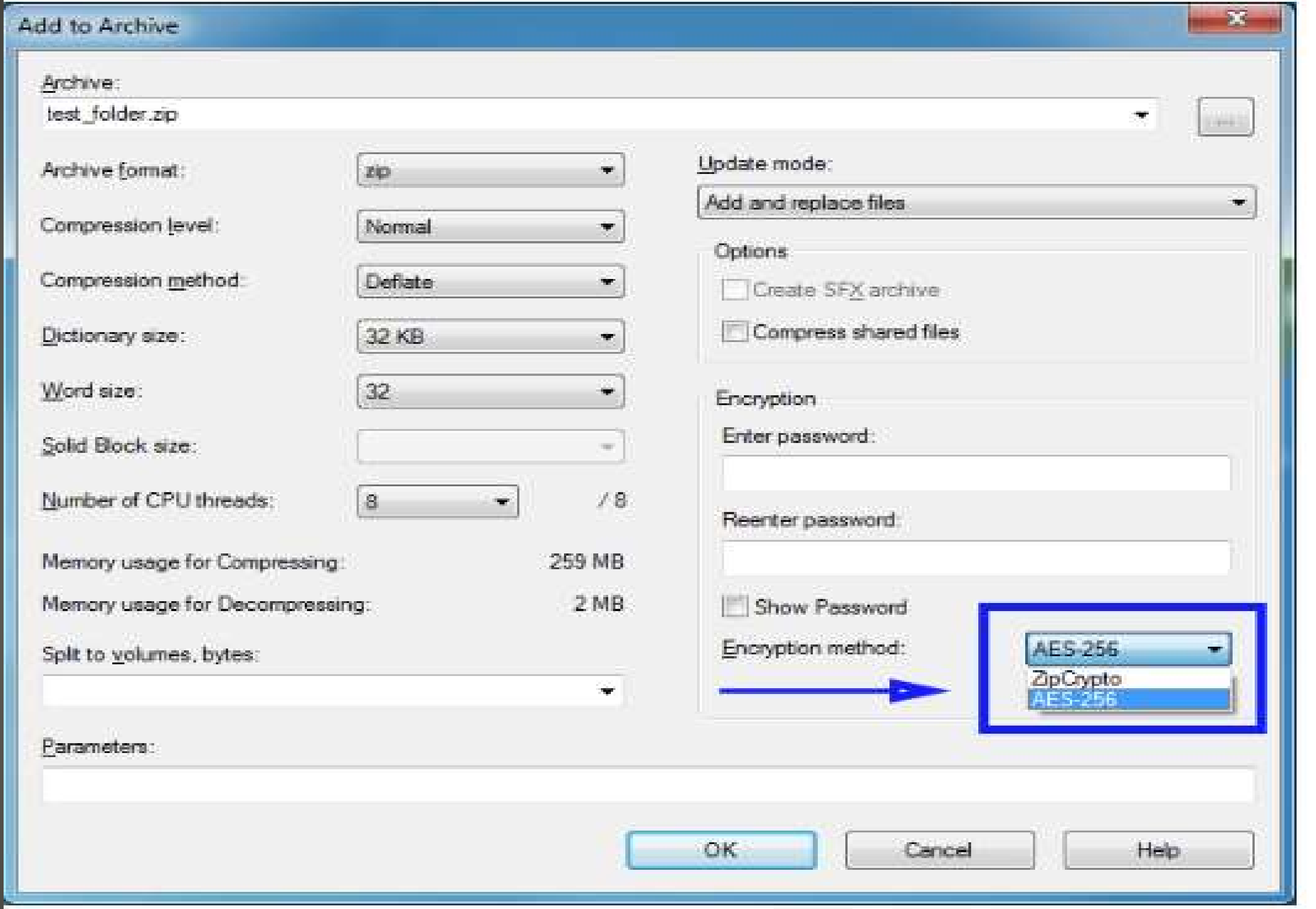
Dictionary size: 32 KB

Update mode: Add and replace files

Options

□ Create SFX archive

□ Compress shared files



Add to Archive

Archive: test_folder.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 8 / 8

Memory usage for Compressing: 259 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Options

□ Create SFX archive

□ Compress shared files

Encryption

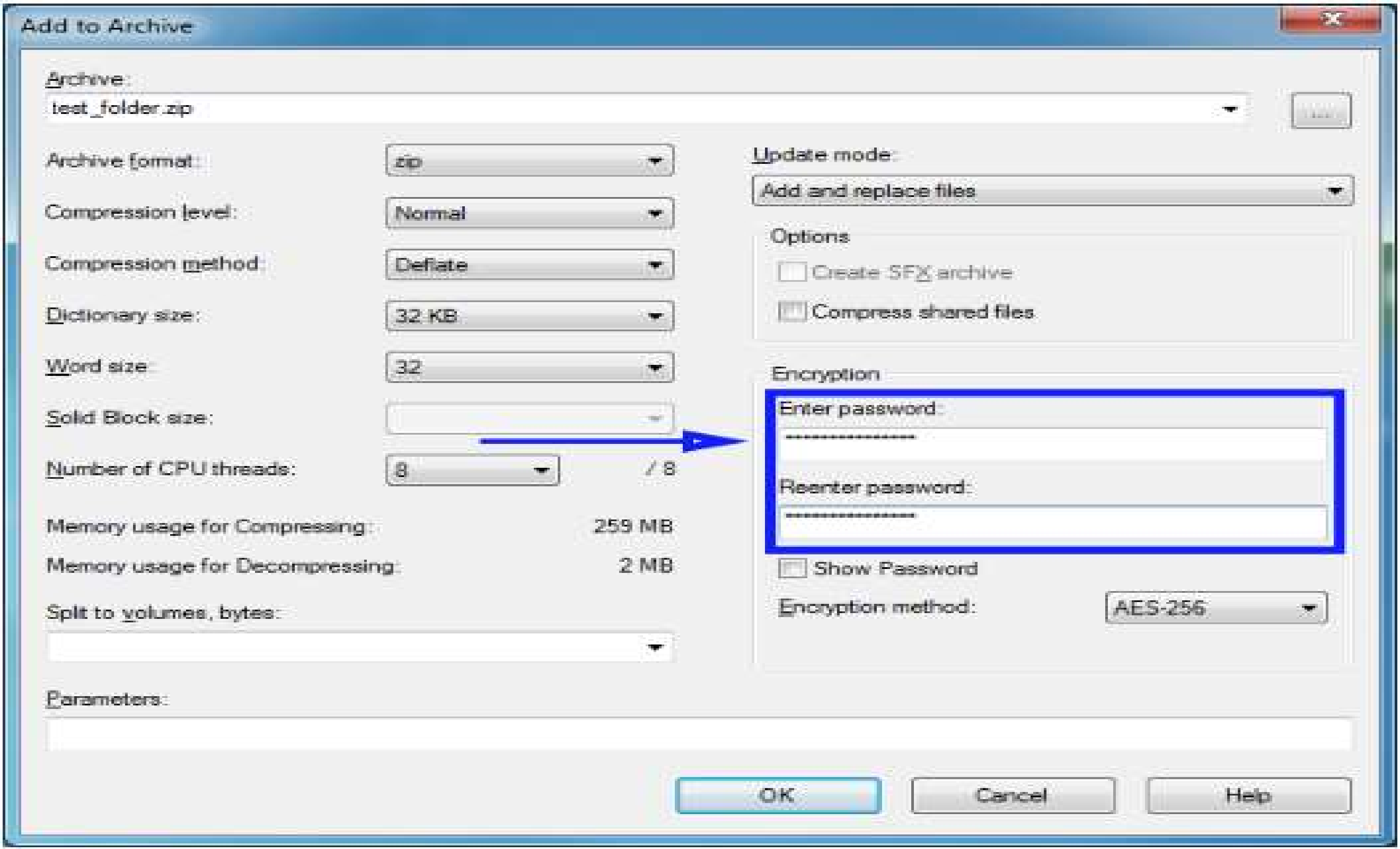
Enter password:

Reenter password:

□ Show Password

Encryption method: AES-256

# 7-Zip



Add to Archive

Archive: test_folder.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 8 / 8

Memory usage for Compressing: 259 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Options

□ Create SFX archive

□ Compress shared files

Encryption

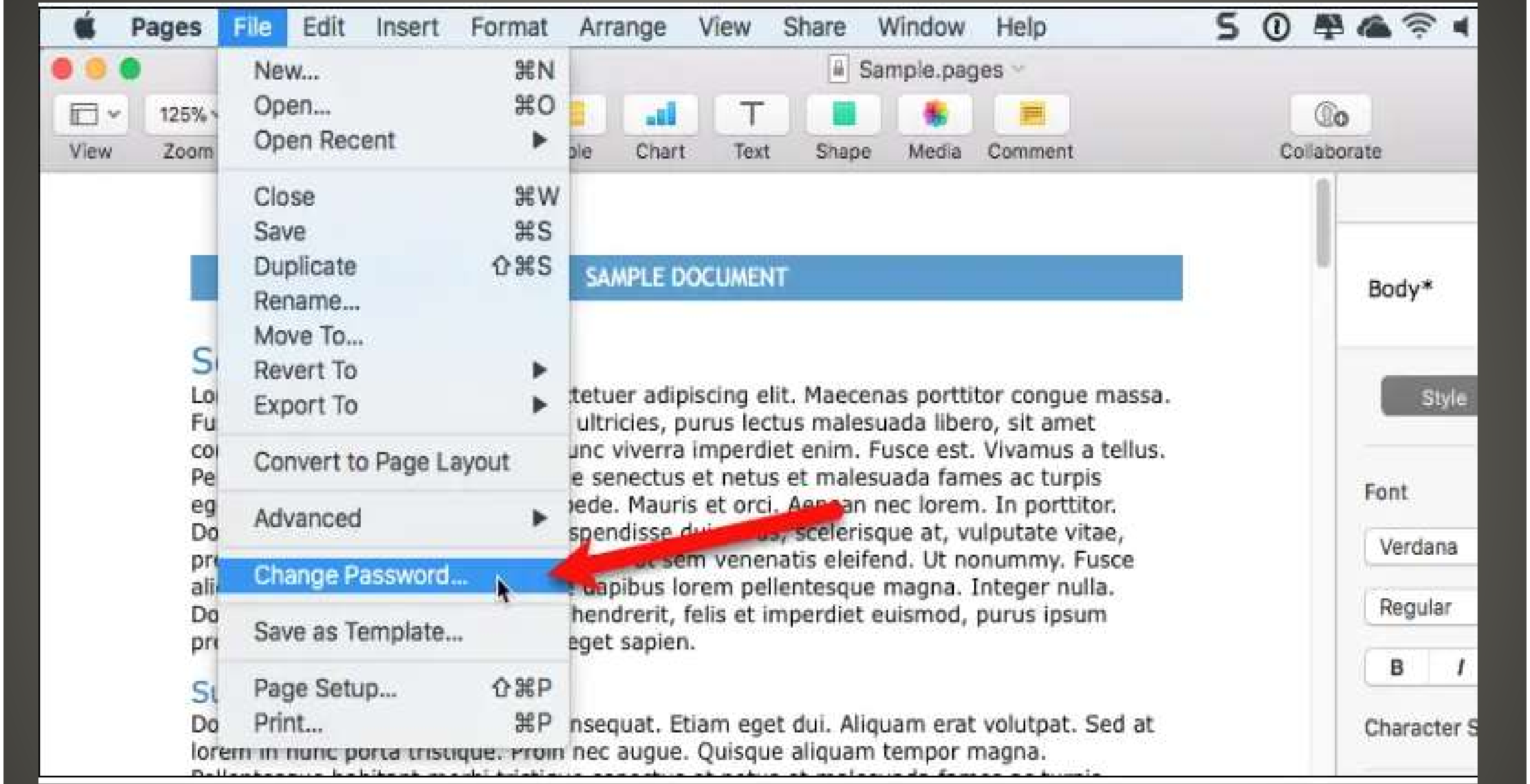
Enter password: ******************

Reenter password: ******************

□ Show Password

Encryption method: AES-256

# 7-Zip

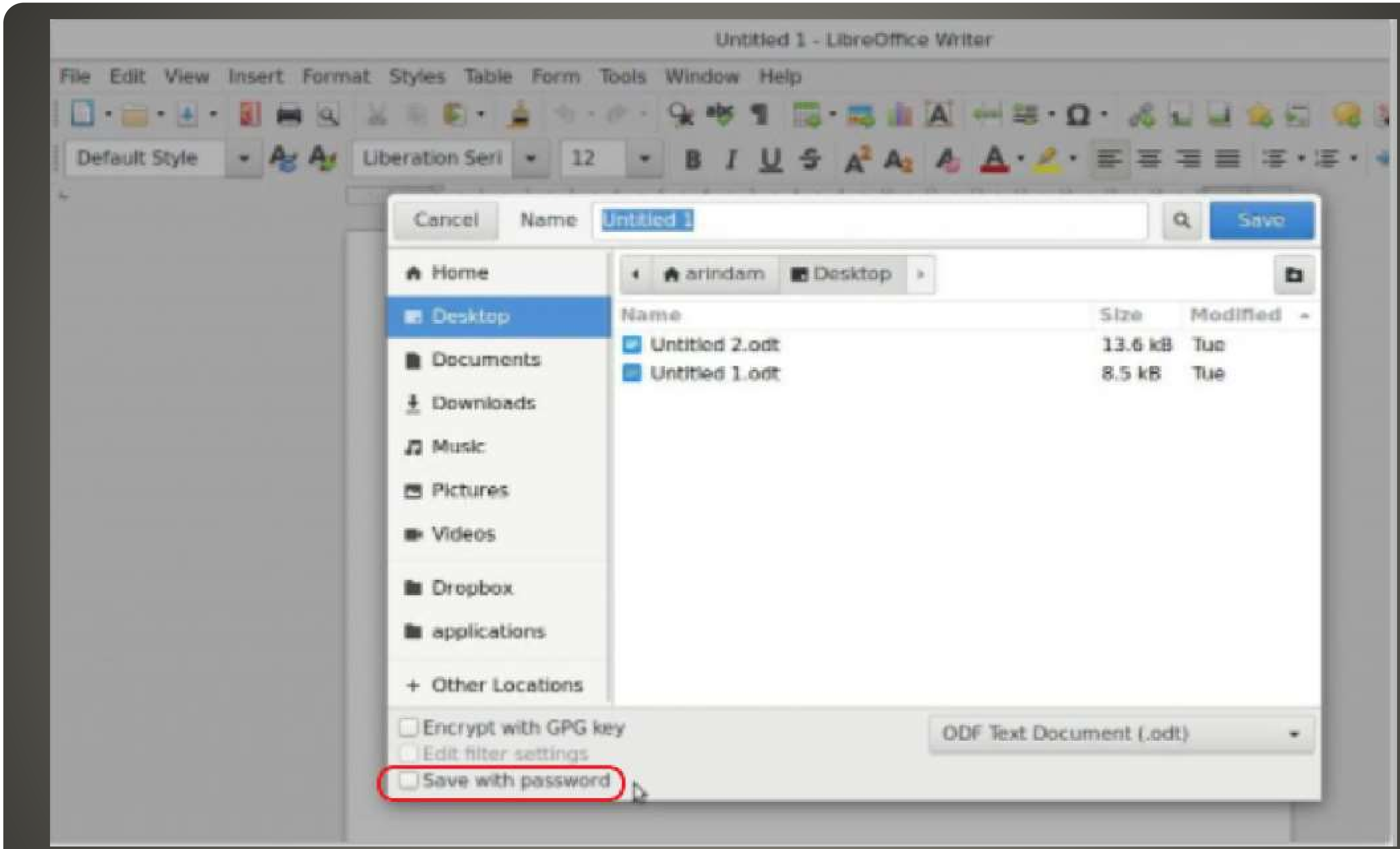


SAMPLE DOCUMENT

Lo tetuer adipiscing elit. Maecenas porttitor congue massa.
Fu ultricies, purus lectus malesuada libero, sit amet
co unc viverra imperdiet enim. Fusce est. Vivamus a tellus.
Pe e senectus et netus et malesuada fames ac turpis
eg pede. Mauris et orci. Aenean nec lorem. In porttitor.
Do spendisse dui us, scelerisque at, vulputate vitae,
pr ut sem venenatis eleifend. Ut nonummy. Fusce
ali dapibus lorem pellentesque magna. Integer nulla.
Do hendrerit, felis et imperdiet euismod, purus ipsum
pr eget sapien.

Do nsequat. Etiam eget dui. Aliquam erat volutpat. Sed at
lorem in nunc porta tristique. Proin nec augue. Quisque aliquam tempor magna.

# But I use a MAC  - Keychain



Name: Untitled 1

| Name | Size | Modified |
|---|---|---|
| Untitled 2.odt | 13.6 kB | Tue |
| Untitled 1.odt | 8.5 kB | Tue |

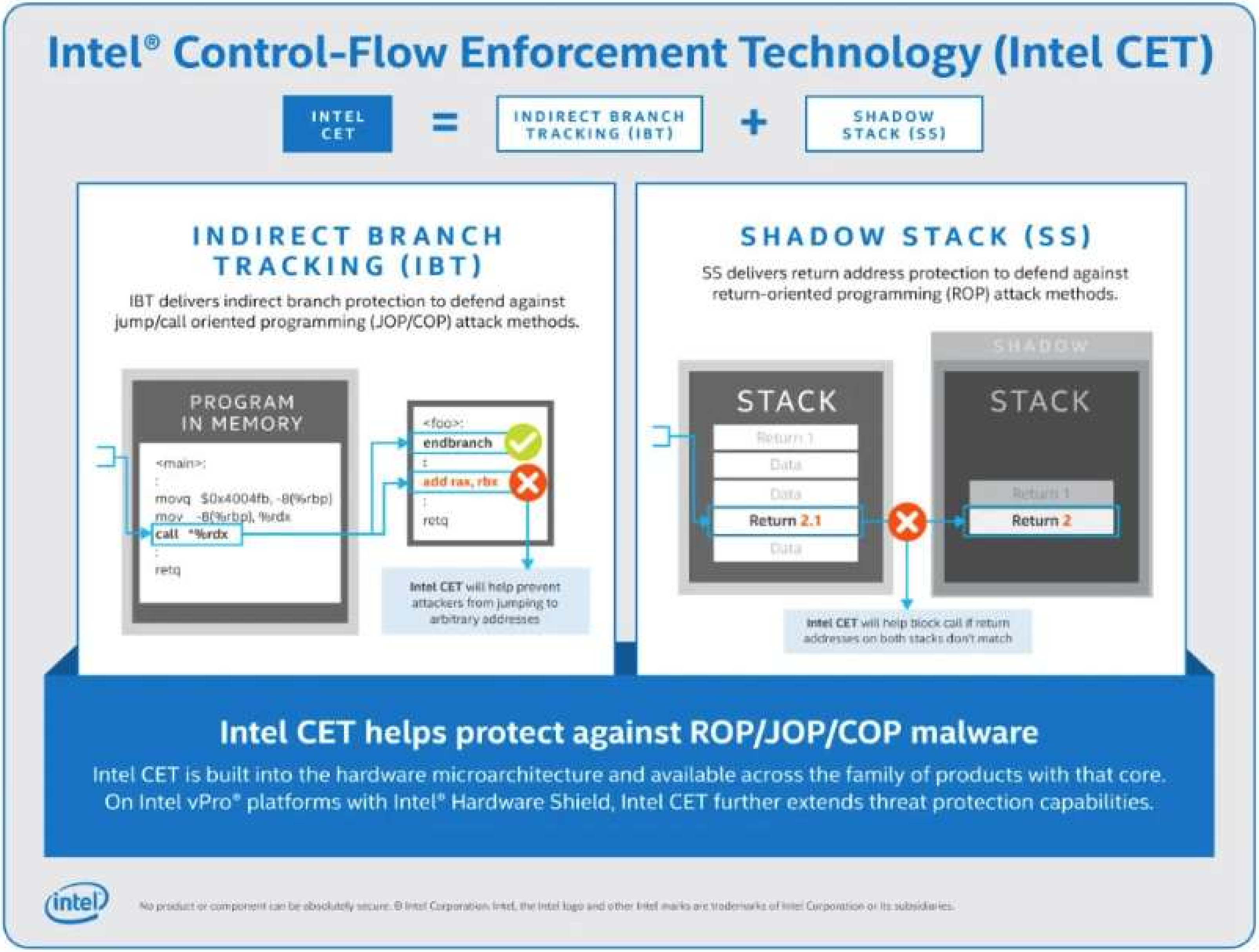
□ Encrypt with GPG key
□ Edit filter settings
□ Save with password

ODF Text Document (.odt)

# Yeah well  LibreOffice?

# Encryption

- Secure PII
- Communicate decryption passphrase out of band
- Consider the disposition of original
- Good practice for use in the Cloud
- TWO EDGED SWORD
- Protection from any/everyone without passcode
- Can include you!



# Intel® Control-Flow Enforcement Technology (Intel CET)

INTEL CET = INDIRECT BRANCH TRACKING (IBT) + SHADOW STACK (SS)

## INDIRECT BRANCH TRACKING (IBT)

IBT delivers indirect branch protection to defend against jump/call oriented programming (JOP/COP) attack methods.

```
<main>:
:
movq   $0x4004fb, -8(%rbp)
mov    -8(%rbp), %rdx
call   *%rdx
:
retq
```

```
<foo>:
endbranch ✓
:
add rax, rbx ✗
:
retq
```

Intel CET will help prevent attackers from jumping to arbitrary addresses

## SHADOW STACK (SS)

SS delivers return address protection to defend against return-oriented programming (ROP) attack methods.

Intel CET will help block call if return addresses on both stacks don't match

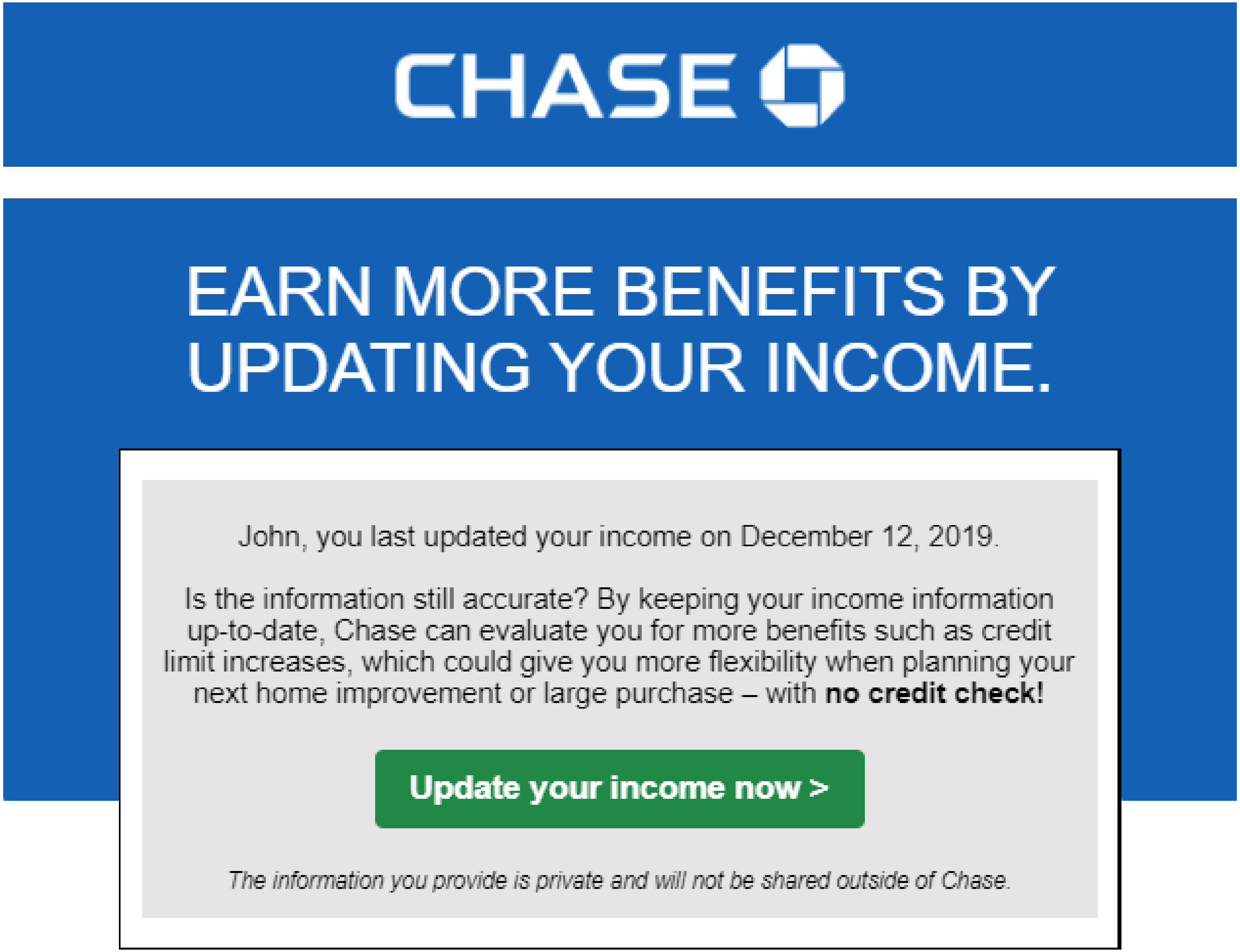
## Intel CET helps protect against ROP/JOP/COP malware

Intel CET is built into the hardware microarchitecture and available across the family of products with that core. On Intel vPro® platforms with Intel® Hardware Shield, Intel CET further extends threat protection capabilities.

Intel CET security feature

- Paper published Queen Mary University
- Radio waves bounced back from subjects
- Heart rate, breath rate, body movements
- Facial recognition and emotion
- Mass detection next

# Thought & emotion research



CHASE

EARN MORE BENEFITS BY UPDATING YOUR INCOME.

John, you last updated your income on December 12, 2019.

Is the information still accurate? By keeping your income information up-to-date, Chase can evaluate you for more benefits such as credit limit increases, which could give you more flexibility when planning your next home improvement or large purchase – with **no credit check!**

*The information you provide is private and will not be shared outside of Chase.*

QUESTIONS ?

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs, Presentations, FirstTime, classes
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

**SCCCCyber@gmail.com**