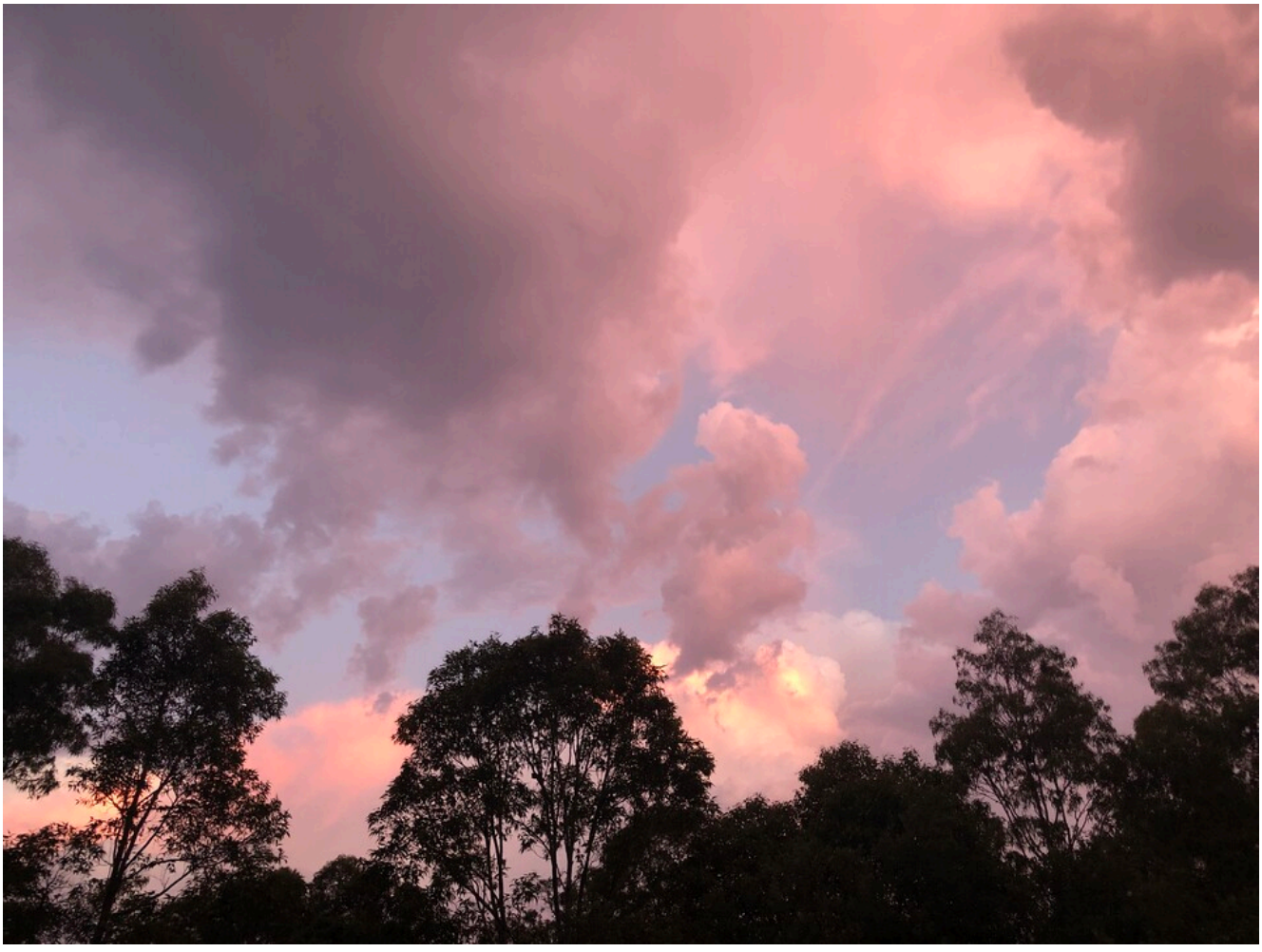
Email Encryption - reducing Your Personal Risks

Published on March 16, 2021



dbcloudart.com (C) 2021

This **first part** of our "Email Encryption" publication explains how the "runaway train" of ransomware attacks and data leaks may ruin **your personal** life and finances.

State of Cybersecurity today

If you look back through DB Cloud Art publications you will see how much we write on the topics of Business Data Protection and *not* paying ransom to cyber criminals. By

the way, we are not alone there.

> *The FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also **encourages** perpetrators to **target more victims** ...*

We wholeheartedly agree with every word in this quote. But, unfortunately, significant number of leaders prefer to "cover things up" and just pay.

> *The dbcloudart.com noticed that, independently of the ransomware attack outcome, there is **one thing in common**: witch-hunt and legal actions to follow.*

In February 2021 the NIST published alarming statistics, stating that c*ybercrime will cost the world $6 trillion annually by 2021* and that ***10% of breached businesses shut down completely***.

Obviously, the failure of business (or significant losses) is always a tragedy for Shareholders and a career challenge for Leadership Team members - therefore attempts to "shift the blame" are made promptly.

Just ... Don't Be That Guy, please!

The reason why we brought all these facts and quotes is simple: in an investigation, following a data breach or ransomware attack, the attempts to "*identify the Directly*

Responsible Individual" will be made. Get ready now - and *being smart about emails* is one of the major tactics!

The Best Email

As we posted recently, *The Best and Safest email is the one you never sent*. This had been proven to be true multiple times and we strongly suggest to "cut down" the volume of your emails.

Do not attach documents, but share them via *internal only* "shared drives" or SharePoint portals etc. (And don't be the person who grants access to others). This gives you the "protection" of enterprise-wide access controls - and necessary audit records, showing who accessed and downloaded what and when.

But what to do if you *have to reply* by email?

The Safe Email

First of all, the **usual rules apply**: your company hopefully provides the tools to encrypt and sign emails with S/MIME certificates, built into your Outlook - **do use them**! These days *every email* must be *at least signed* (so nobody can "put words into your mouth" later), and ideally you would want to *encrypt every email* you send. *Avoid attachments* at all costs. *If you have to attach - do encrypt*!

But what if your organisation does not provide personal S/MIME certificates?

> *How can you get sure that it's not your email that will be pointed at later as the source of data leak?*

This is where you have to "think out of the box" a bit and challenge yourself mentally. Yes, the steps below will increase your load and they will complicate (but just a bit) your "daily workflow". But this is the price you need to pay for your own safety. And, besides, it is always good to "flex your brain muscles" - mental activity seems to delay Alzheimer's.

Protect your messages - yourself!

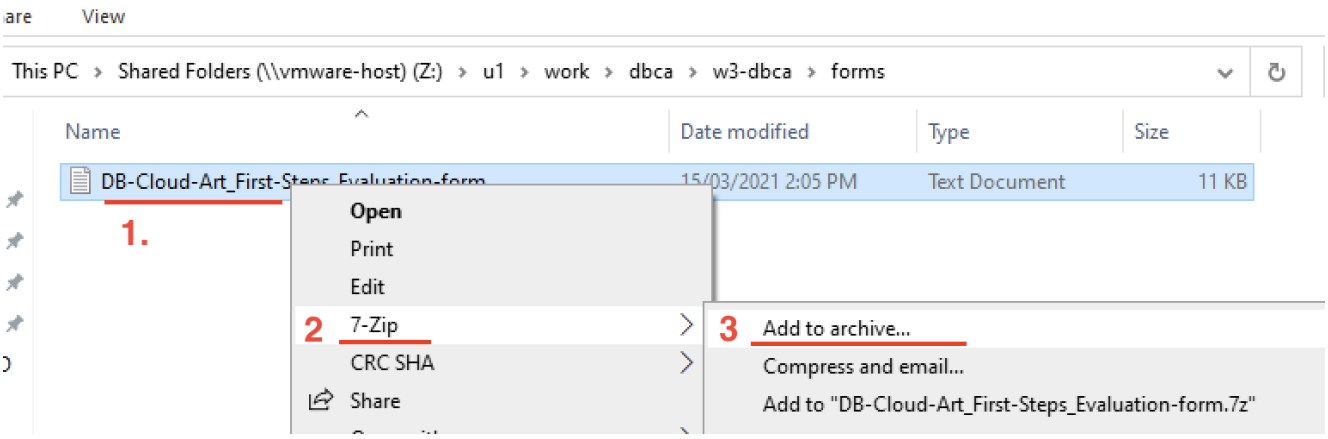
You can always protect *yourself* a bit more - but please do *check your local country's encryption laws,* are you actually allowed to use encryption? If you can't - don't send important emails. As simple as that.

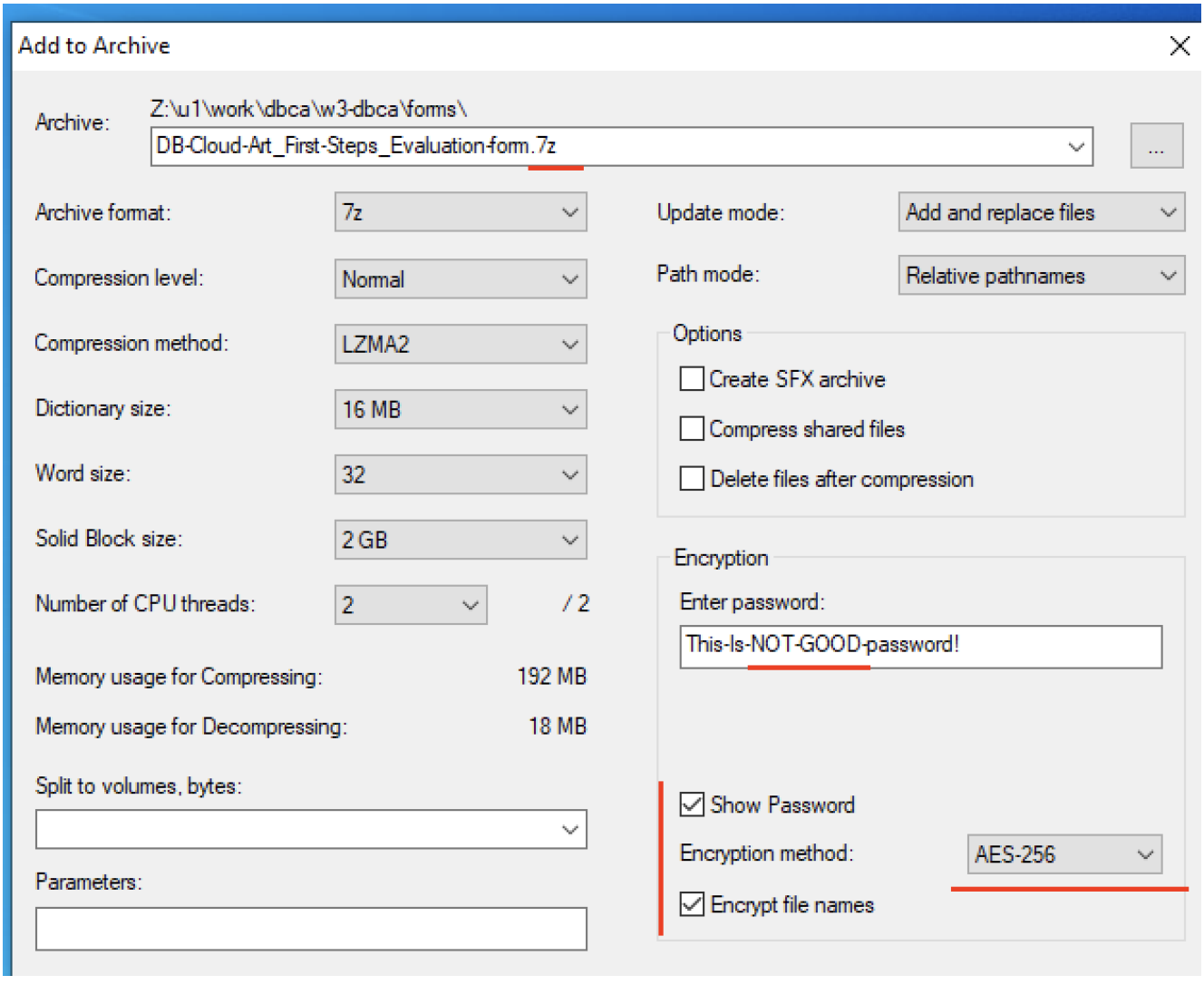
The basic way of DIY email protection is *encrypting the document locally* on your computer and *then* sharing it, *already encrypted*. (You may use this approach even for the files, placed on shared drive - and sure for those, attached to emails).

Most probably, you already have "7-Zip" archiver, installed on your computer. (If not - you can always request it from your Enterprise Software Archive or install directly from project website).

The steps are very simple:

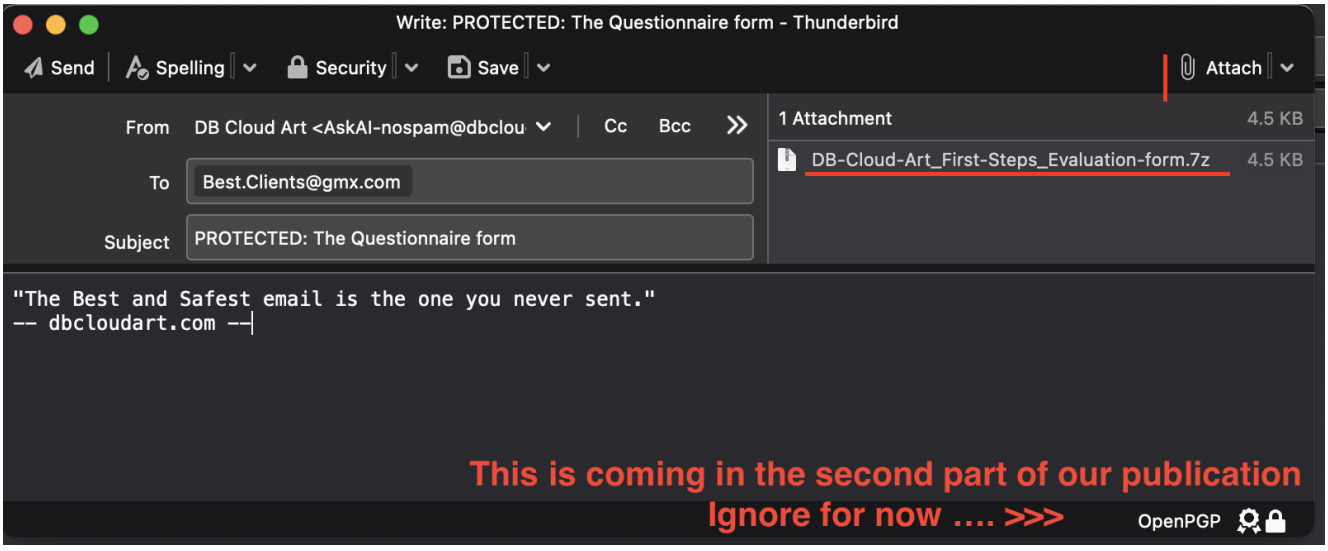
- Find your document, "right click" it, choose to archive with 7-Zip and select *AES-256 encryption of resulting file*.



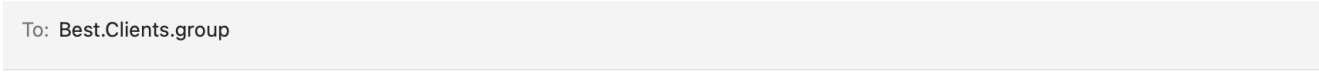


- Choose *strong passwords* - and this is *extremely important*! Here is the good example and tool to generate them. *Do not use same password* multiple times.

- Attach the encrypted file to email and send it. *Do not list the password in the email*!



- Using one of "secure messaging" platforms (i.e. iMessage, Signal and similar) chat the password to your recepient. *Do not share password and encrypted message by same communication channel.*



- Ideally, you may pre-create the "passwords schedule" and *share it in person* with your recipient (another great excuse to have lunch or drinks together!)

cruyEtA7	*(charlie - romeo - uniform - yankee - ECHO - tango - ALPHA - Seven)*
pRuhEs8E	*(papa - ROMEO - uniform - hotel - ECHO - sierra - Eight - ECHO)*
B8xeRaF6	*(BRAVO - Eight - x-ray - echo - ROMEO - alpha - FOXTROT - Six)*
xuV4CAc7	*(x-ray - uniform - VICTOR - Four - CHARLIE - ALPHA - charlie - Seven)*
7EtHefre	*(Seven - ECHO - tango - HOTEL - echo - foxtrot - romeo - echo)*
3hEza9ef	*(Three - hotel - ECHO - zulu - alpha - Nine - echo - foxtrot)*
6Ra2ejAT	*(Six - ROMEO - alpha - Two - echo - juliet - ALPHA - TANGO)*
KaXeya4u	*(KILO - alpha - X-RAY - echo - yankee - alpha - Four - uniform)*
tRU5Huma	*(tango - ROMEO - UNIFORM - Five - HOTEL - uniform - mike - alpha)*
spava6AN	*(sierra - papa - alpha - victor - alpha - Six - ALPHA - NOVEMBER)*
Gejaz6ch	*(GOLF - echo - juliet - alpha - zulu - Six - charlie - hotel)*
xeCHa8uv	*(x-ray - echo - CHARLIE - HOTEL - alpha - Eight - uniform - victor)*
ruFrez8D	*(romeo - uniform - FOXTROT - romeo - echo - zulu - Eight - DELTA)*
HaswE6Ud	*(HOTEL - alpha - sierra - whiskey - ECHO - Six - UNIFORM - delta)*
ja9uMaca	*(juliet - alpha - Nine - uniform - MIKE - alpha - charlie - alpha)*
7atRA3AN	*(Seven - alpha - tango - ROMEO - ALPHA - Three - ALPHA - NOVEMBER)*

The general idea is *for both sides to cross out used passwords immediately* and go to the next one, until fresh sheet is necessary (and one more round of drinks is coming up).

And please remember: most probably *all your emails and encrypted attachments will be read by some "agencies" anyway* - today, next month or in years. We do not know for sure when, but we do know it will happen. So be very

sensible about what you send and attach ...

Let's Practice ...

On our website we offer our clients simple IT Security assessment form. It can be used as realistic target for secure emailing exercise - and *we will even reply* if you fill that form in, encrypt it and send to us! (Please don't forget to text us the password for your encrypted archive - our phone number is listed on our website as well and you may look it up in all major encrypted chat applications).

Needless to say, the *questions in that questionnaire are real* and we may produce the actual report for you - you can read all details in that text file ...

Now you may ask: "*why to use that poorly looking Text file*"? According to Cisco, Microsoft **Office formats** such as Word, PowerPoint and Excel make up the **most** prevalent group of **malicious file** extensions at **38%** of the total. Please keep it in mind. We are quickly getting back to those times when even HTML-formatted emails may be rejected.

Let's exchange some secure emails now ... We will be waiting!

Allow us at #**dbcloudart** help you, our details are on **dbcloudart.com**, let's schedule a no obligation call with your leadership team.

Our **“Data Survival Plan”** might become that “safety escape” for your business!

Stay safe!

Disclaimer

The information contained in this document is for general information purposes only. The information is provided by "DB Cloud Art Pty. Ltd." and while we endeavor to keep the information up to date and correct, we make no representations or warranties of any kind, expressed or implied, about this document completeness, accuracy, reliability and suitability for any purpose. Any reliance you place on such information is therefore strictly at your own risk. In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this document.