Malicious Emails

How to Identify Them and How to Protect Yourself

presented by **Rappahannock IT**

SECURITY | SUPPORT | INFRASTRUCTURE | CLOUD

RAPPAHANNOCK IT

1. Identify the Sender

This is the first thing you should do whenever you receive an email, especially if:

- It is requesting sensitive information
- It asks you to click a link
- It contains an attachment

Did you verify my email address before clicking the link to this slideshow?

RAPPAHANNOCK IT

1. Identify the Sender

nick@youritcompany.net

This is the **most important** portion of an email address: the portion after the @ symbol.

It's called the domain and *usually* you can trust it to tell you where an email came from.

In some cases though, you can't. We'll cover how to identify those situations later.

---

nick@yourltcompany.net

Notice the lowercase "L" disguised as an "i"

An attacker may attempt to mislead you with a domain designed to *look* legitimate.

Can you identify the problem with this email address?

RAPPAHANNOCK IT

1. Identify the Sender

nick@yourtechsupport.com

Attackers will often use domains that *sound* legitimate, when in reality they have no association with the company they're pretending to represent.

Some examples

help@microsoft-techsupport.biz	vs	**help@microsoft.com**
support@dropbox-usa.net	vs	**support@dropbox.com**
info@googlefinancialpartners.com	vs	**info@google.com**

1. Identify the Sender

nick@youritcompany.net

Attackers will also try to make this portion misleading in an attempt to fool you.

---

microsoftsupport@yahoo.com

irs-fraud@frauddepartment.ru

Don’t fall victim to spoofs like this.

RAPPAHANNOCK IT

Always

verify the sender

If you identify a fraudulent email, report it to your IT department immediately

RAPPAHANNOCK IT

2. Screen the Links

OK, so you've verified the sender as someone legitimate.

This does not mean that you're free to explore any content they've sent you.

RAPPAHANNOCK IT

2. Screen the Links

Emails can contain **links** to malicious websites, or **attachments** with malware disguised as documents.

malware is an umbrella term for things like **viruses**, **ransomware**, and **spyware**

Often times when an attacker has gained access to an email account, the attacker will attempt to compromise each of the victim's contacts as well.

What if ***your*** contact has had their email account compromised? By clicking a link or downloading an attachment, you could be walking into a trap without even knowing it.

or what if the domain has been **spoofed** and the sender looks like someone from your organization?

RAPPAHANNOCK IT

2. Screen the Links

Website links have **two** parts:

- A web address
- A picture or display text

Attackers will often use display text to disguise a malicious web address.

http://google.com/

They can also use pictures or buttons, so be on your toes

Track Package

RAPPAHANNOCK IT

2. Screen the Links

These Links...	...Could Actually Be These Links
Click Here to Track Your Package	http://www.ransomware-download.com/
https://www.yourbank.com/	http://www.stealyourpassword.net/
wikipedia.org	http://www.illegalstuff.info/

RAPPAHANNOCK IT

2. Screen the Links

Hover Over Your Links

If you hover over a link with your mouse, you will be told exactly where the link wants to take you.

It works whether you're on a Mac or a PC.

It works whether you're in Outlook or in Chrome.

It will work almost anywhere you see a link to a website.

Sometimes it will pop up in a box next to your cursor.

Sometimes it will pop up in the corner of your screen.

But it will pop up somewhere - look for it.

2. Screen the Links

Identify the Domain

Similar to a fraudulent email address, you'll want to verify the **domain** of the website you're being linked to.

It will tell you where you're actually going.

So how do you identify the domain of a website?

RAPPAHANNOCK IT

2. Screen the Links

First, anything preceding **://** can be ignored

The **domain** is the last portion of what's left. It is made up of the final two segments surrounding the final dot

http://www.mydomain.com/home-page.html

We can also ignore anything after the first forward slash

RAPPAHANNOCK IT

2. Screen the Links

Can You Identify the Domain?

http://google.trustworthy.biz/	trustworthy.biz
http://drive.google.com/my-document.doc	google.com
http://netflix.com/s4909sHTHS4802s!thjmod=4	netflix.com
http://www.microsoft.com.pc-hosting.ru/	pc-hosting.ru
bankofamerica.online.silverfish.net	silverfish.net
en.wikipedia.org/wiki/Main_Page	wikipedia.org
Messenger.facebook.hostbin.com	hostbin.com
www.qooqle.com	qooqle.com

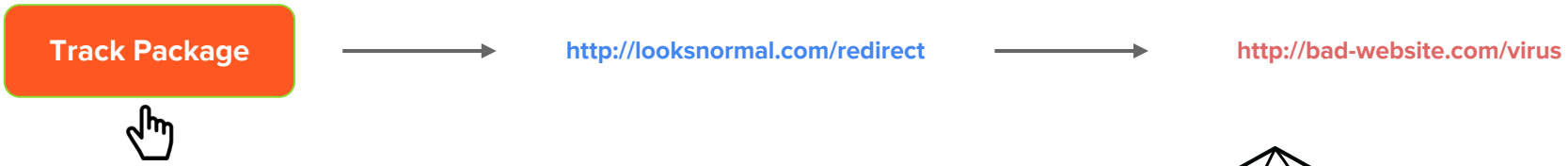
Attackers will try to mislead you with website domains too.

RAPPAHANNOCK IT

2. Screen the Links

Unlike an email address, website domains **cannot** be faked.

They can **redirect** you though, so be careful.



RAPPAHANNOCK IT

Always

check the domain

If you don’t recognize a website, don’t visit it.

3. Don't Trust Attachments

You should NEVER open an email attachment blindly

By simply clicking it, you could compromise your security and risk spreading the attack to your peers.

The safest precaution you can take is to identify the **type** of file it contains.

Every file has a type, and you can tell what that is by its **file extension**.

RAPPAHANNOCK IT

3. Don't Trust Attachments

Here are some familiar file extensions:

.doc	.docx	Word Document
.xls	.xlsx	Excel Spreadsheet
.ppt	.pptx	PowerPoint
	.pdf	PDF
	.txt	Text File

Similar to the **.com** or **.net** of a domain, the file extension will be that last portion of the file name.

RAPPAHANNOCK IT

3. Don't Trust Attachments

Here are some more file extensions:

		.exe	Executable
		.bat	Windows Script
		.js	JavaScript
.docm	.xlsm	.pptm	Office Document with Macros

These extensions are called executables and are normal too.

The difference is that they can make your computer perform specific actions.

Put another way, they can control your computer.

This is why you should always ensure you trust an executable's source - **verify what it is and where it came from.**

RAPPAHANNOCK IT

3. Don't Trust Attachments

If you receive an executable in an email attachment, you should assume it is malware

3. Don't Trust Attachments

Attackers will attempt to disguise file types

Just like with domains

august-sales-numbers.exe

invoice324.pdf.exe

fedexshippinglabel.bat

sales-projections.xlsx.js

Always

screen attachments

If you don’t recognize a file type, don’t open it.

Example

This is an actual malicious email

David, a friend of mine, has had his account compromised. Posing as David, the attacker has sent me this message intended to gain my confidence.

Let's examine it.

From: Schwarz, David <[redacted].COM>
Sent: Thursday, July 6, 2017 2:49 PM
Subject: Please View DAVID___SCHWARZ Article Documents.pdf

DocuSign

David Schwarz sent you a document to review.

David Schwarz
[redacted].com

Please review the attached. I stumbled on the attached article this morning and you suddenly bumped into my mind so I thought it would only be nice of me to share.
Please share your thoughts when you're able to view the document.
Cheers to you,
Dave

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

Alternate Signing Method
Visit DocuSign.com, click 'Access Documents', and enter the security code:
B0E5D0C4C8604AA5B36C968E3B05453C2

About DocuSign
Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe -- DocuSign provides a professional trusted solution for Digital Transaction Management™.

Questions about the Document?
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly or replying to this email.

If you are having trouble signing the document, please visit the Help with Signing page on our Support Center.

Download the DocuSign App

This message was sent to you by dawn dickinson who is using the DocuSign Electronic Signature Service. If you would rather not receive email from this sender you may contact the sender with your request.

Here we have what appears to be a personalized message from David

Does this sound like David?

Am I expecting an email like this from David?

From: Schwarz, David <[redacted].COM>
Sent: Thursday, July 6, 2017 2:49 PM
Subject: Please View DAVID___SCHWARZ Article Documents.pdf

DocuSign

David Schwarz sent you a document to review.

David Schwarz
[redacted].com

Please review the attached. I stumbled on the attached article this morning and you suddenly bumped into my mind so I thought it would only be nice of me to share.
Please share your thoughts when you're able to view the document.
Cheers to you,
Dave

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

Alternate Signing Method
Visit DocuSign.com, click 'Access Documents', and enter the security code:
B0E5D0C4C8604AA5B36C968E3B05453C2

About DocuSign
Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe -- DocuSign provides a professional trusted solution for Digital Transaction Management™.

Questions about the Document?
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly or replying to this email.

If you are having trouble signing the document, please visit the Help with Signing page on our Support Center.

Download the DocuSign App

This message was sent to you by dawn dickinson who is using the DocuSign Electronic Signature Service. If you would rather not receive email from this sender you may contact the sender with your request.

Notice the attempts to legitimize the appearance of the email.

From: Schwarz, David <[redacted].COM>
Sent: Thursday, July 6, 2017 2:49 PM
Subject: Please View DAVID___SCHWARZ Article Documents.pdf

DocuSign

David Schwarz sent you a document to review.

David Schwarz
[redacted].com

Please review the attached. I stumbled on the attached article this morning and you suddenly bumped into my mind so I thought it would only be nice of me to share.
Please share your thoughts when you're able to view the document.
Cheers to you,
Dave

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

Alternate Signing Method
Visit DocuSign.com, click 'Access Documents', and enter the security code:
B0E5D0C4C8604AA5B36C968E3B05453C2

About DocuSign
Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe -- DocuSign provides a professional trusted solution for Digital Transaction Management™.

Questions about the Document?
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly or replying to this email.

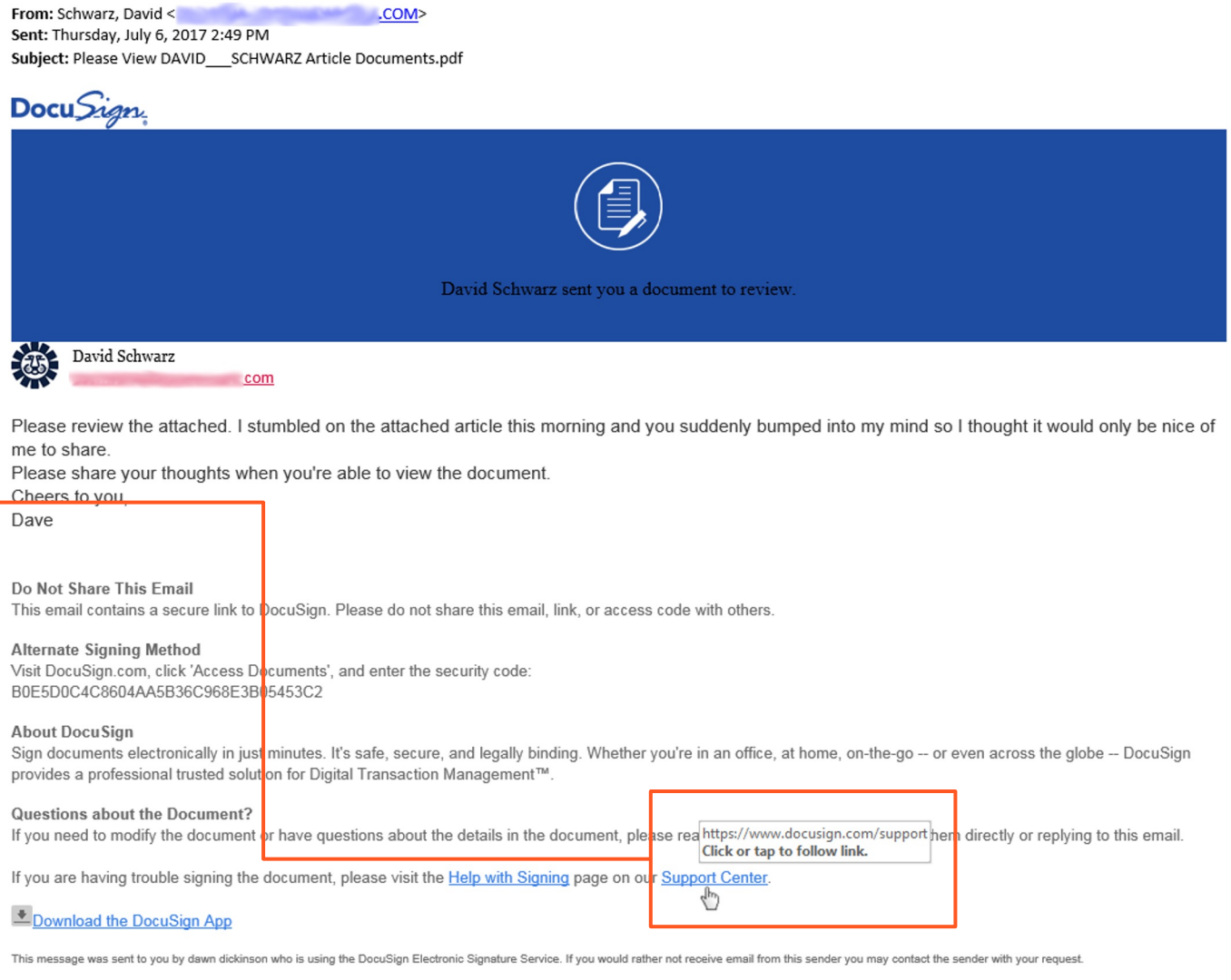
If you are having trouble signing the document, please visit the Help with Signing page on our Support Center.

Download the DocuSign App

This message was sent to you by dawn dickinson who is using the DocuSign Electronic Signature Service. If you would rather not receive email from this sender you may contact the sender with your request.

It even contains legitimate links to further disguise itself.

Don't forget to hover!



From: Schwarz, David <[redacted].COM>
Sent: Thursday, July 6, 2017 2:49 PM
Subject: Please View DAVID___SCHWARZ Article Documents.pdf

DocuSign

David Schwarz sent you a document to review.

David Schwarz
[redacted].com

Please review the attached. I stumbled on the attached article this morning and you suddenly bumped into my mind so I thought it would only be nice of me to share.
Please share your thoughts when you're able to view the document.
Cheers to you,
Dave

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

Alternate Signing Method
Visit DocuSign.com, click 'Access Documents', and enter the security code:
B0E5D0C4C8604AA5B36C968E3B05453C2

About DocuSign
Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe -- DocuSign provides a professional trusted solution for Digital Transaction Management™.

Questions about the Document?
If you need to modify the document or have questions about the details in the document, please rea https://www.docusign.com/support hem directly or replying to this email.
Click or tap to follow link.

If you are having trouble signing the document, please visit the Help with Signing page on our Support Center.

Download the DocuSign App

This message was sent to you by dawn dickinson who is using the DocuSign Electronic Signature Service. If you would rather not receive email from this sender you may contact the sender with your request.

From: Schwarz, David <[redacted].COM>
Sent: Thursday, July 6, 2017 2:49 PM
Subject: Please View DAVID___SCHWARZ Article Documents.pdf

DocuSign

David Schwarz sent you a document to review.

David Schwarz
[redacted].com

Please review the attached. I stumbled on the attached article this morning and you suddenly bumped into my mind so I thought it would only be nice of me to share.
Please share your thoughts when you're able to view the document.
Cheers to you,
Dave

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

Alternate Signing Method
Visit DocuSign.com, click 'Access Documents', and enter the security code:
B0E5D0C4C8604AA5B36C968E3B05453C2

About DocuSign
Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe -- DocuSign provides a professional trusted solution for Digital Transaction Management™.

Questions about the Document?
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly or replying to this email.

If you are having trouble signing the document, please visit the Help with Signing page on our Support Center.

Download the DocuSign App

This message was sent to you by dawn dickinson who is using the DocuSign Electronic Signature Service. If you would rather not receive email from this sender you may contact the sender with your request.

Be on the lookout for inconsistencies

Assessment

Immediately this email raises suspicion.

- David's never used Docusign before.
- David would never use phrasing like "bumped into my mind."
- Aren't articles usually links to websites? I've never received one as an attachment before.
- Why would a signing service host an article anyway?
- Who is Dawn Dickinson and why does it say she sent this message?

At this point you should report this email to your IT department, and ignore anything it asks you to do.

You should also contact David via some method other than email to figure out if he actually sent this, or if he's been compromised.

RAPPAHANNOCK IT

Assessment

This email appears to have an attachment as well.

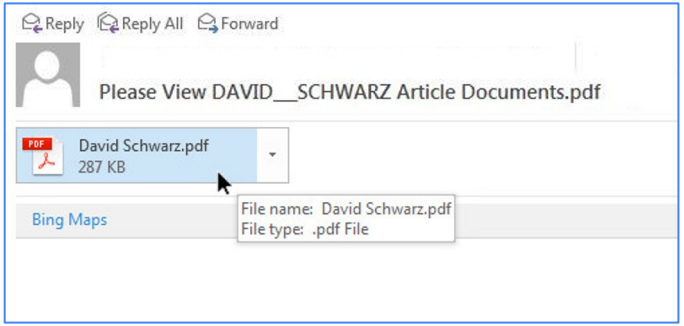
We've already determined this email is a threat. At no point should you open it.

RAPPAHANNOCK IT

Assessment

By examining the attachment we can **confirm** it is a PDF file.

We will investigate it here purely for demonstration.

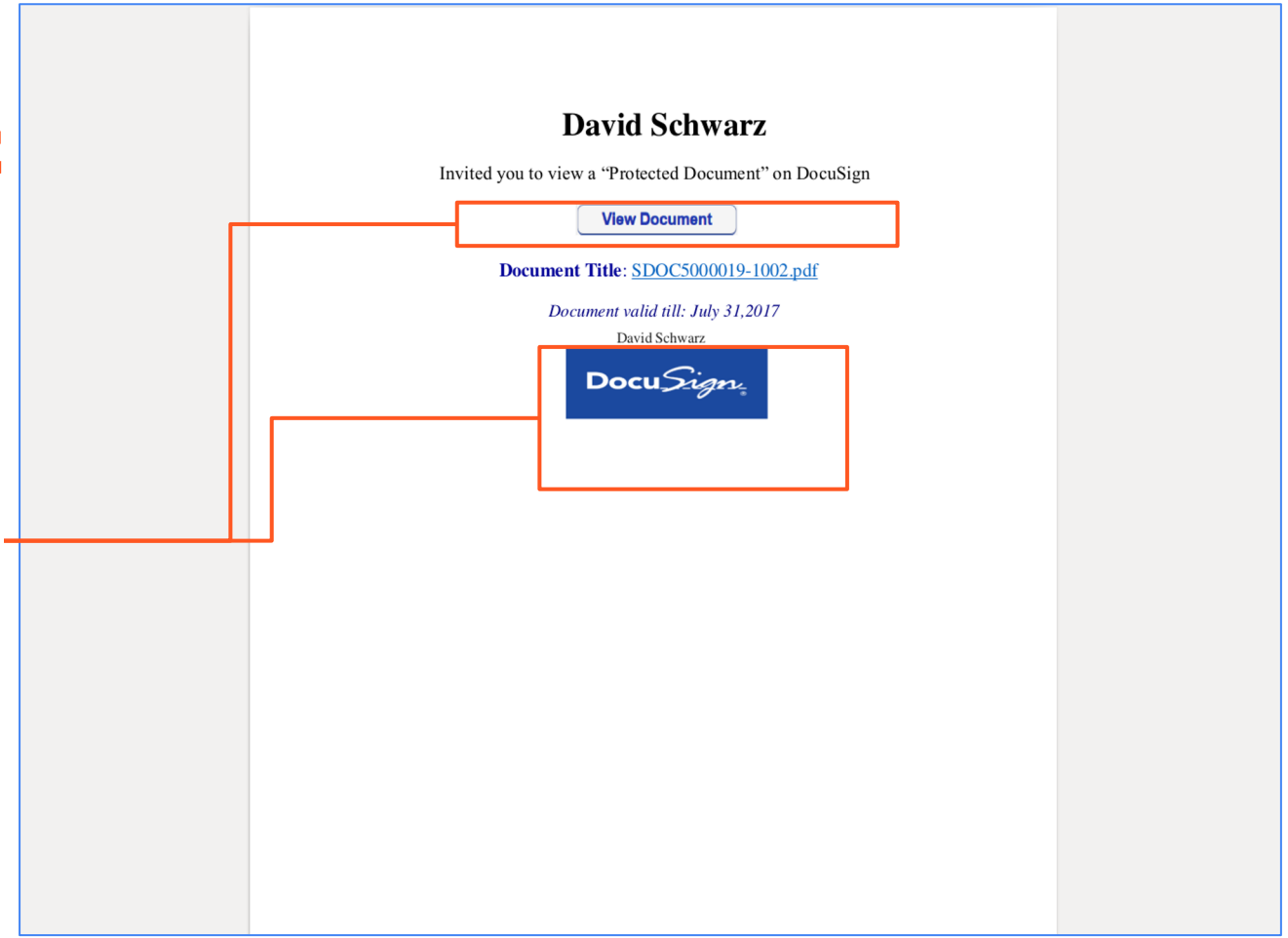


RAPPAHANNOCK IT

Assessment

This is our attachment

More attempts to legitimize the appearance.



RAPPAHANNOCK IT

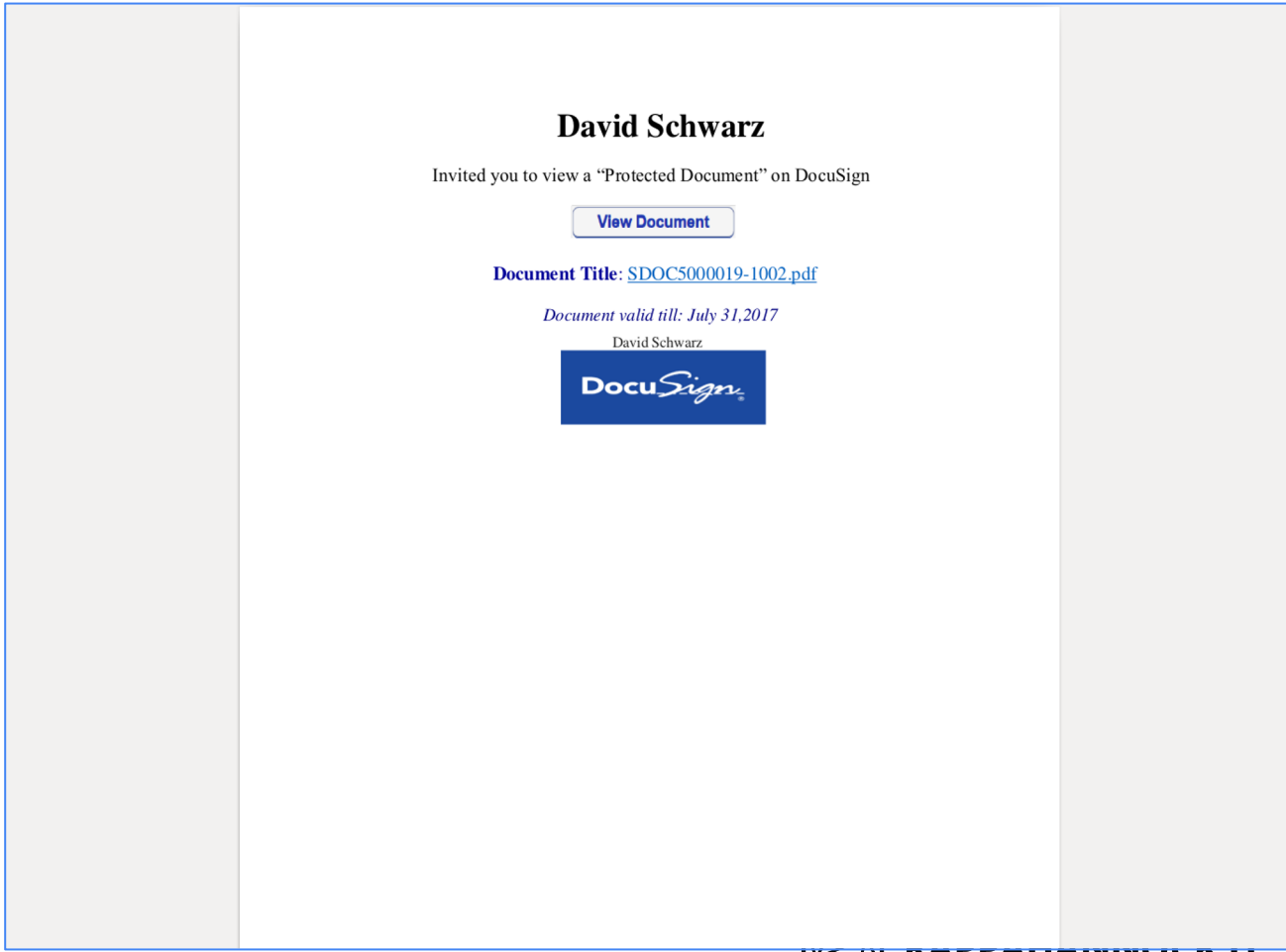
Assessment

This is our attachment

This particular attack is sneaky.

It hides a malicious link inside of a harmless PDF, instead of putting it directly in the email body.

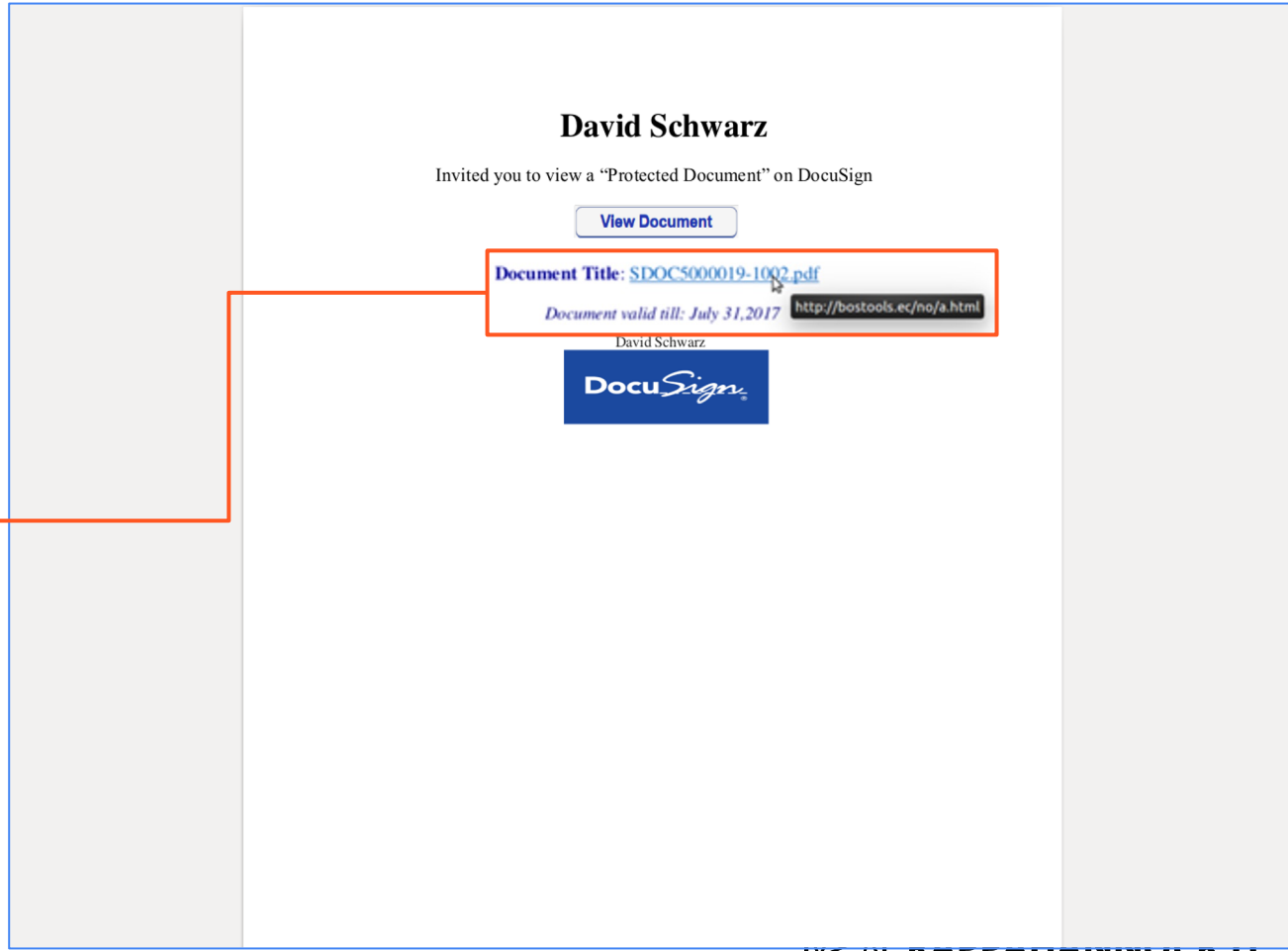
This way it's able to bypass my spam filter.



Assessment

This is our attachment

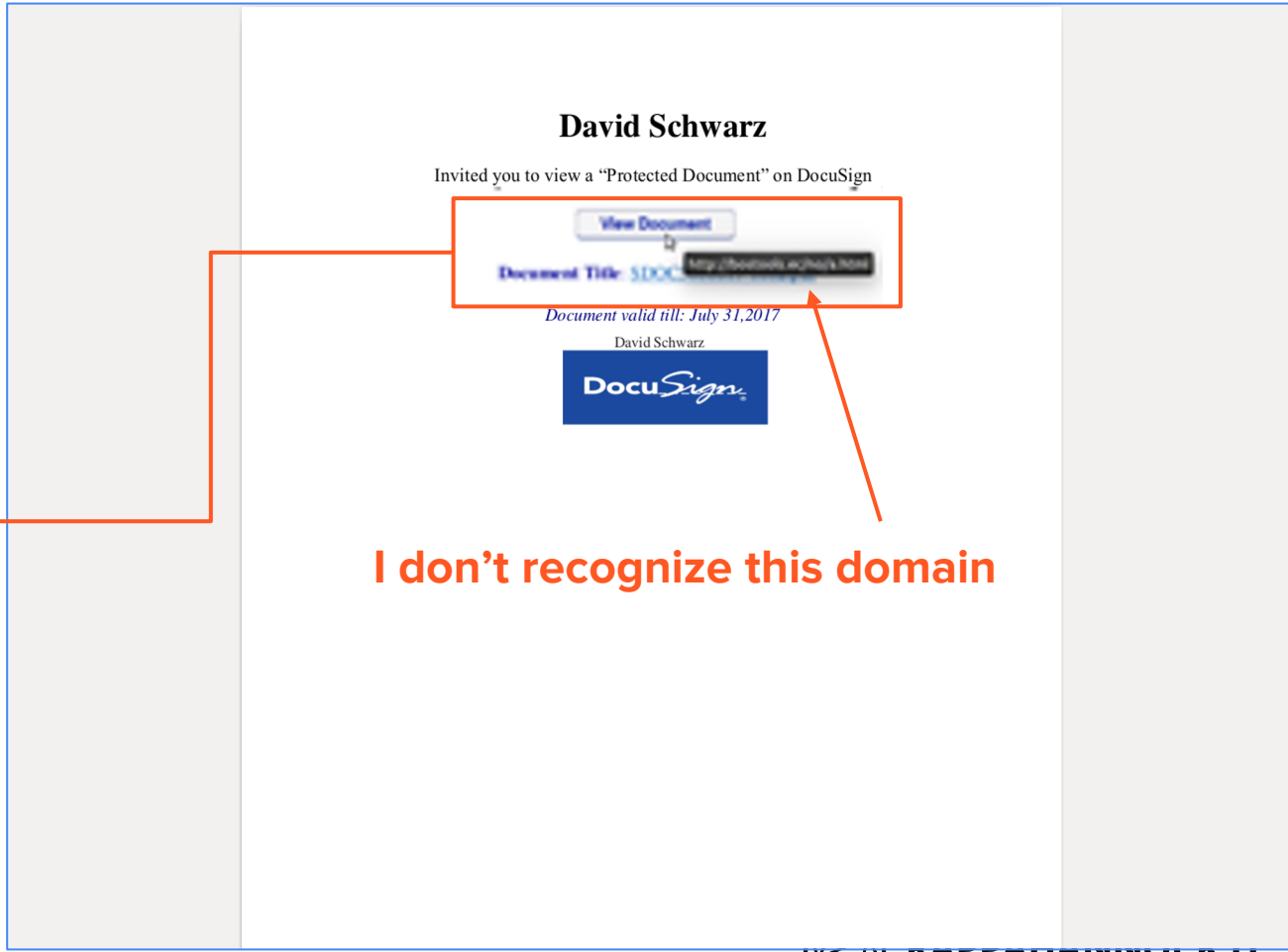
By hovering, we can see where these links actually take us.



Assessment

This is our attachment

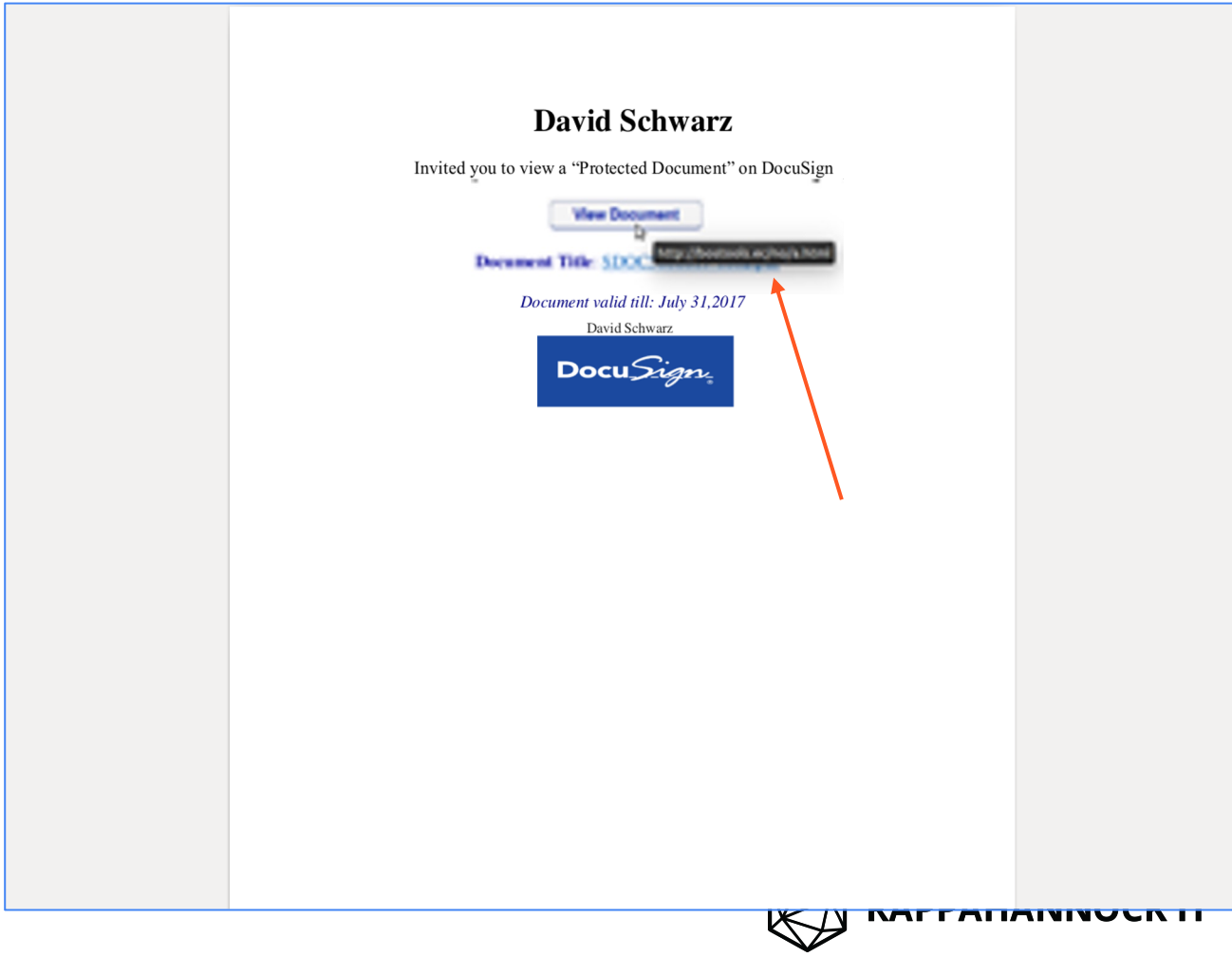
By hovering, we can see where these links actually take us.



Assessment

Under no circumstances should you click those links.

By this point you should have already reported this email to your IT department.

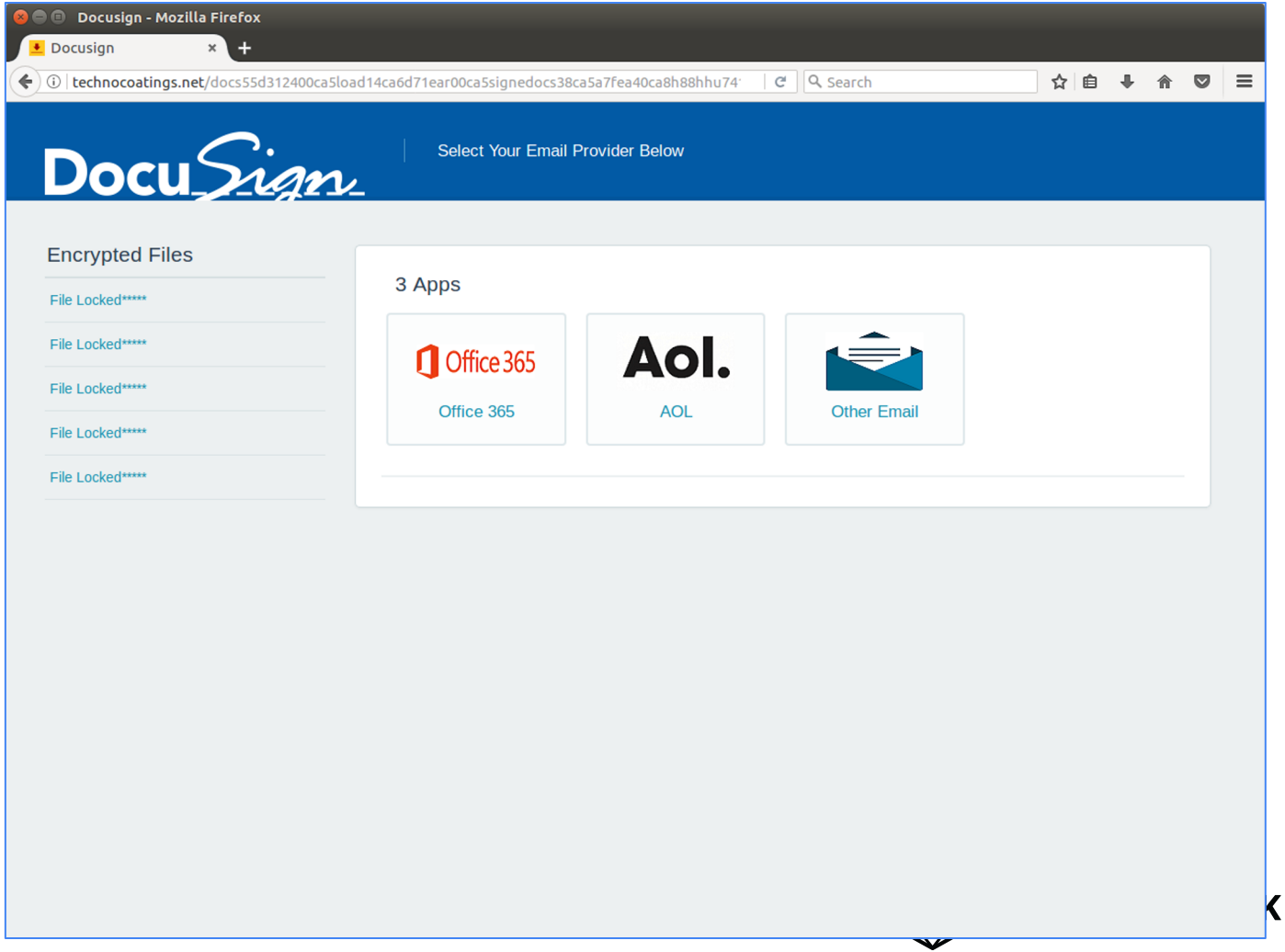


Assessment

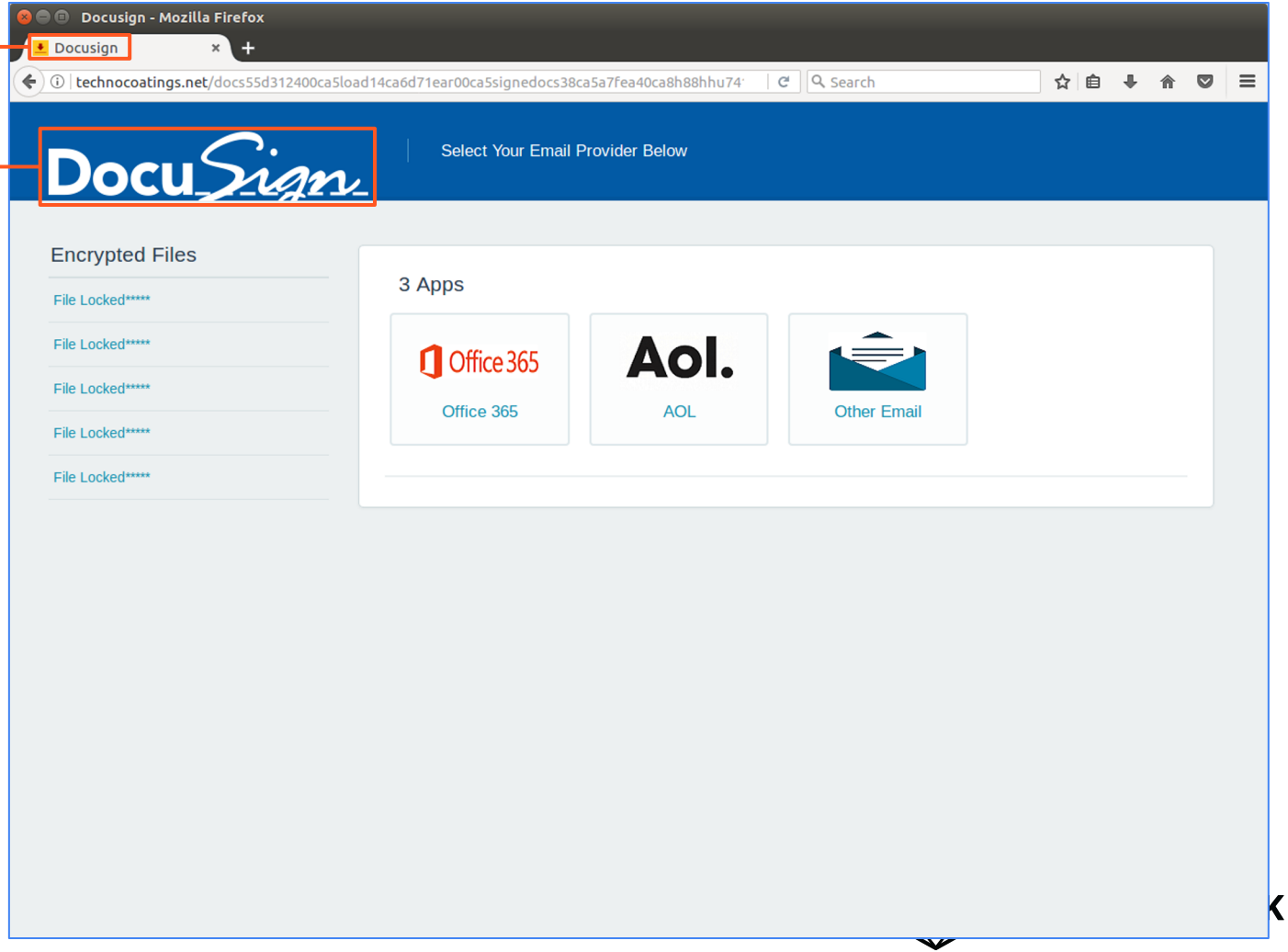
I will open this link for demonstrational purposes.

Do not attempt this on your own.

This is where the link takes us.



Notice how this website is posing as Docusign.com



K IT

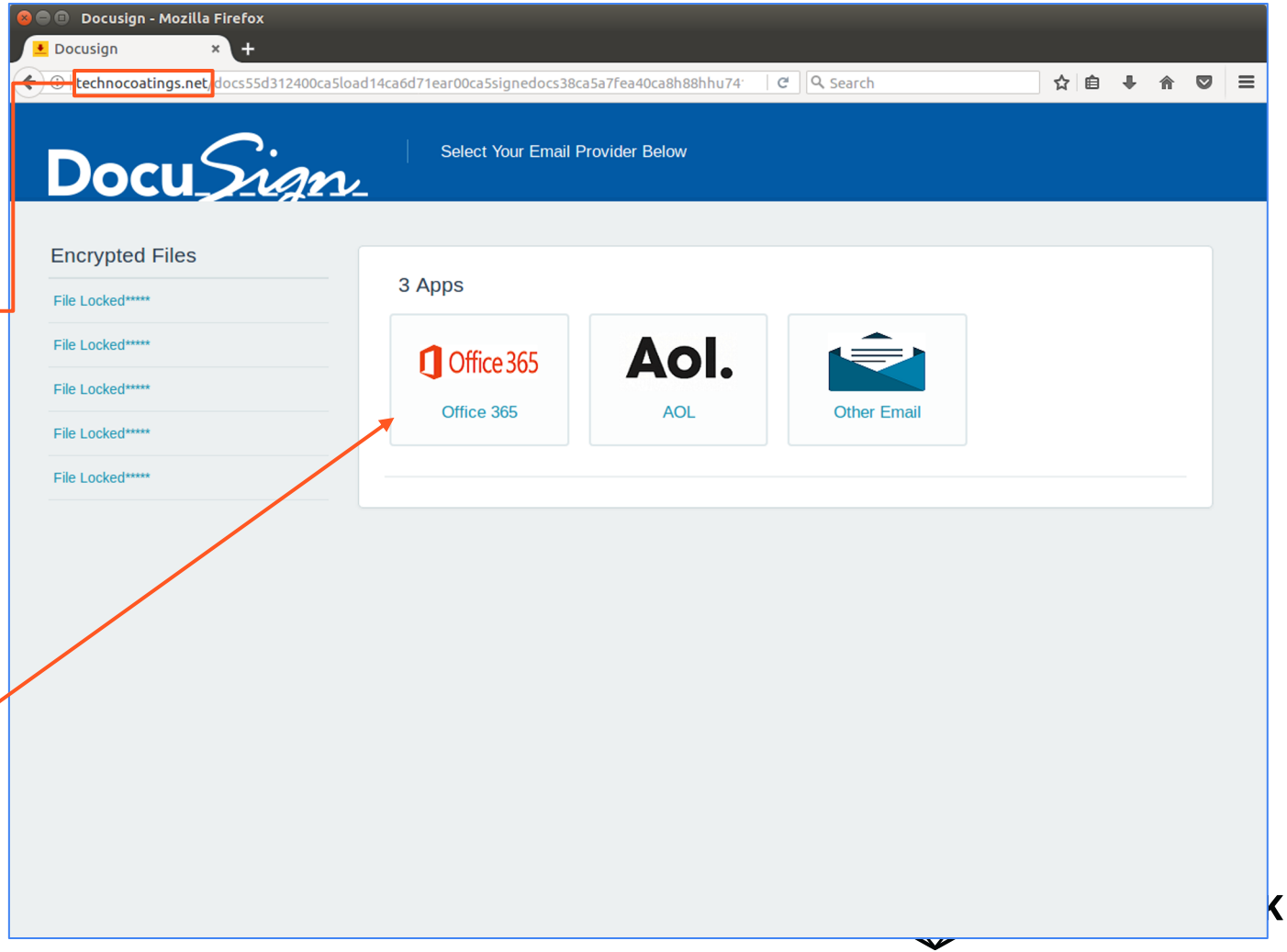
By examining the domain, however, we can see otherwise

We also see that bostools.ec (the domain linked in the attachment) redirected us to technocoatings.net

Remember links can **redirect** you to different destinations.

This is why it is important to evaluate the legitimacy of an email.

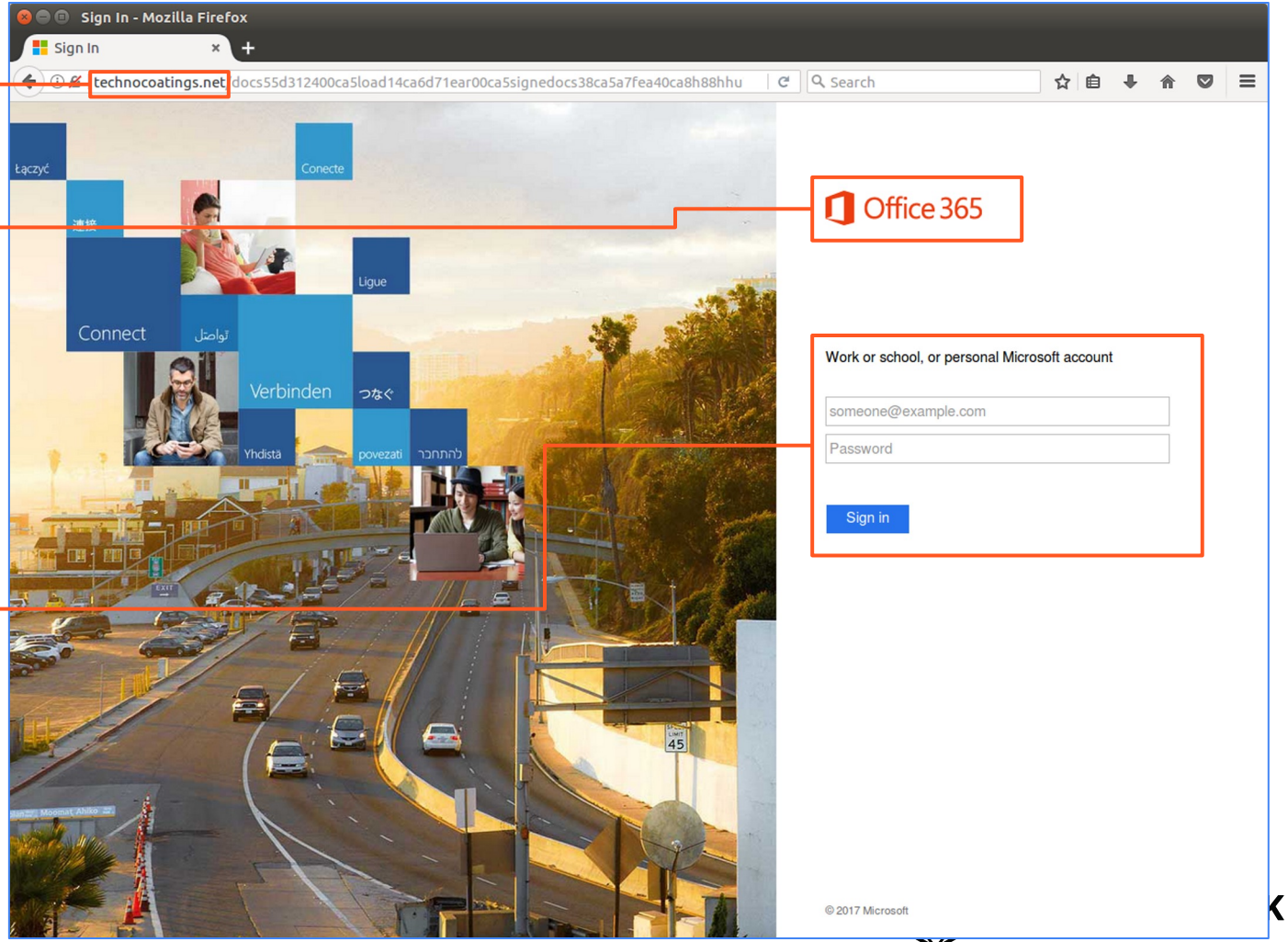
By clicking this button here, I'm taken to the following page...



Again, we see an illegitimate domain

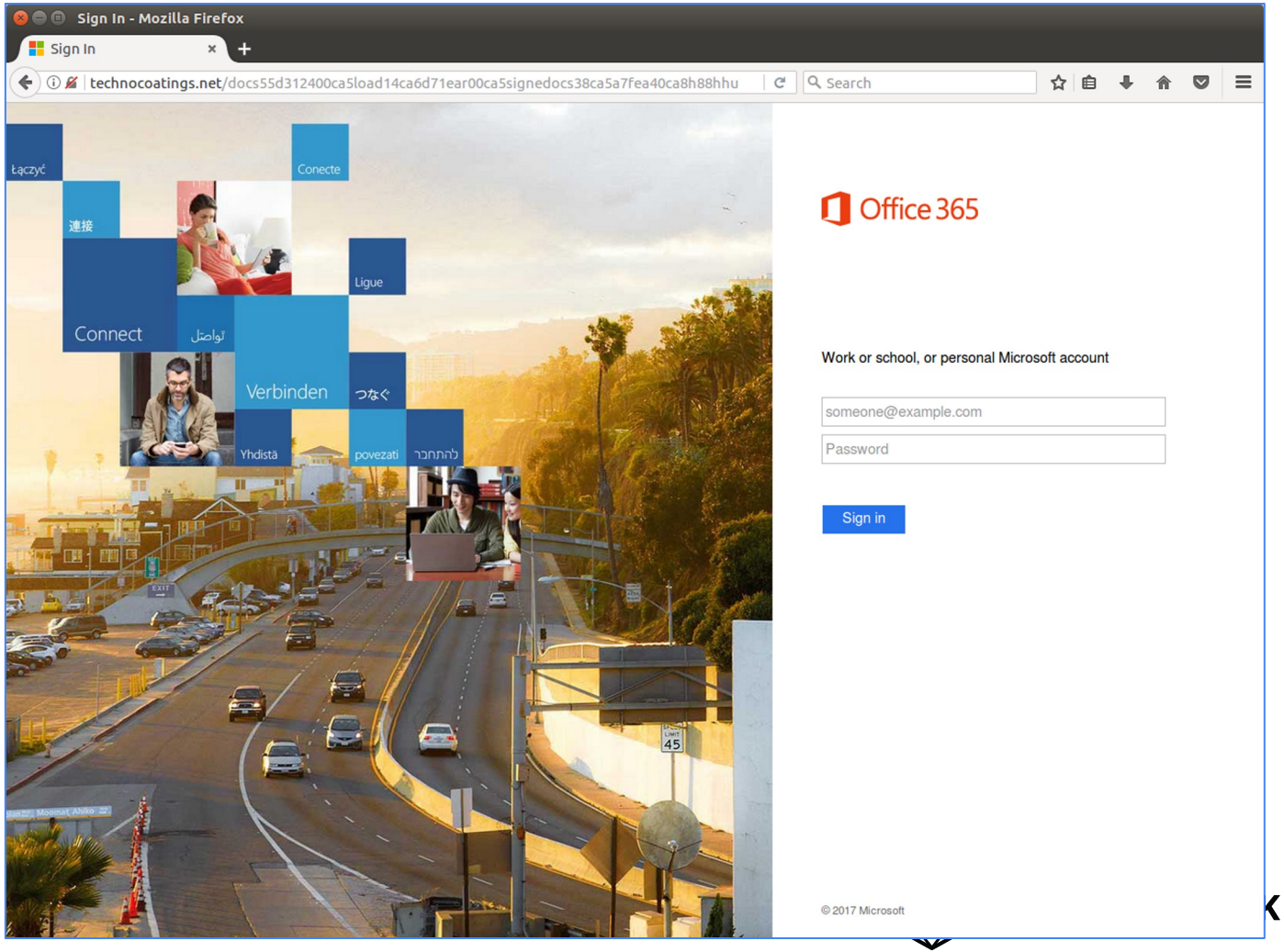
Yet it is disguised as a Microsoft login page

Were you to enter your login information here, you would be giving the attacker your email address and password



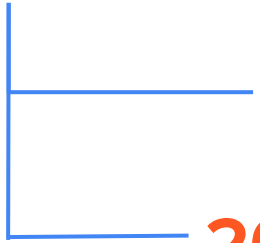
This is called
phishing.

There are thousands of these attacks circulating through email at any given moment.



Just to give you an idea

Between January and March of 2022



289,371 — New phishing websites discovered

20 million — New malware strains discovered

$1.6 million — Average cost of a phishing attack

Sources

http://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf

https://blog.cloudmark.com/2022/01/13/survey-spear-phishing-a-top-security-concern-to-enterprises/

RAPPAHANNOCK IT

Don’t Be a Victim

1. Identify the sender
2. Screen the links
3. Don’t trust attachments

Report anything suspicious to your IT department. They are paid to ensure your company’s security.

RAPPAHANNOCK IT

Security Products Help

but they only get you so far

The most effective safety measure is you

RAPPAHANNOCK IT