Take All my Money!

Advanced Spear Phishing Attacks

David Wind
@slashcrypto
ITSECX 2019

About me

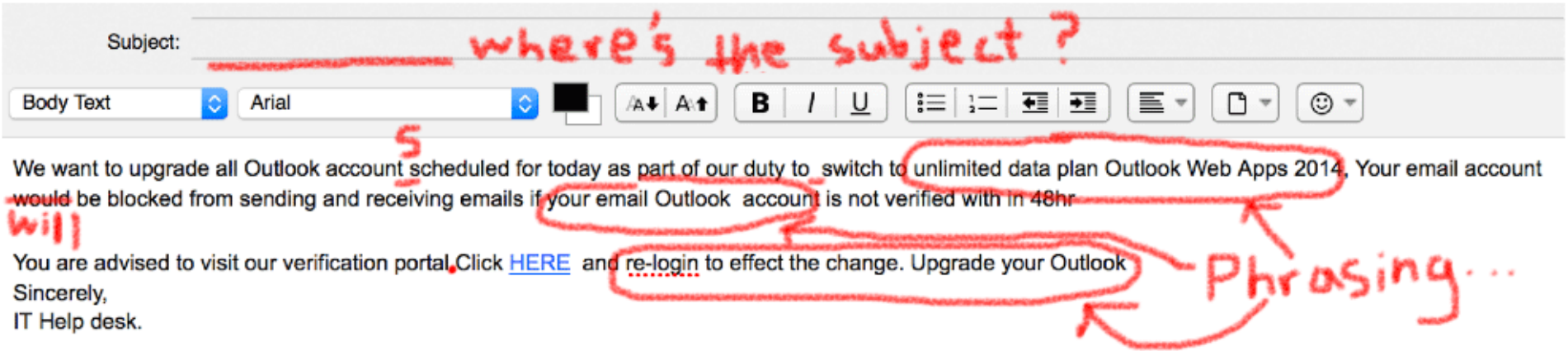
- David Wind (David.Wind@a1.digital)
- Security Consultant / Penetration Tester / Social Engineer @A1 Digital
- Privacy enthusiast and bug bounty hunter
  - Acknowledgments: Microsoft, Google, Netflix, XING and others
- @slashcrypto
- slashcrypto.org

A1 Digital

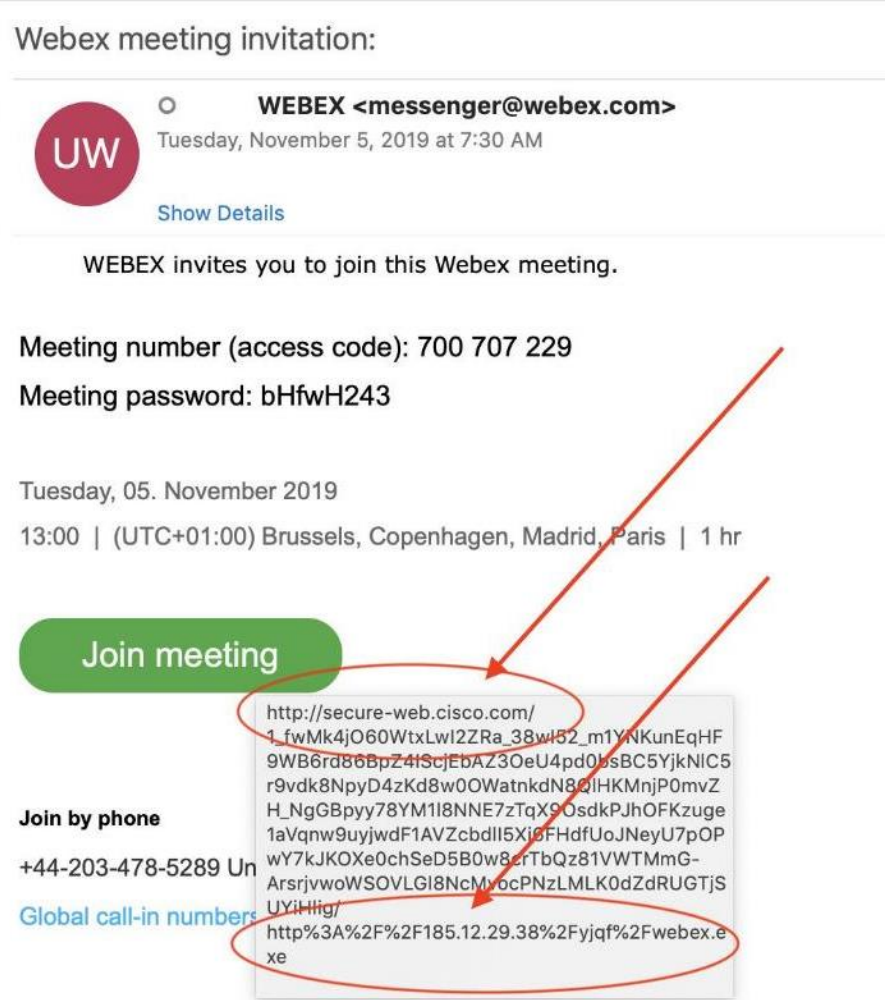
A1 Digital

Phishing Emails

A1 Digital



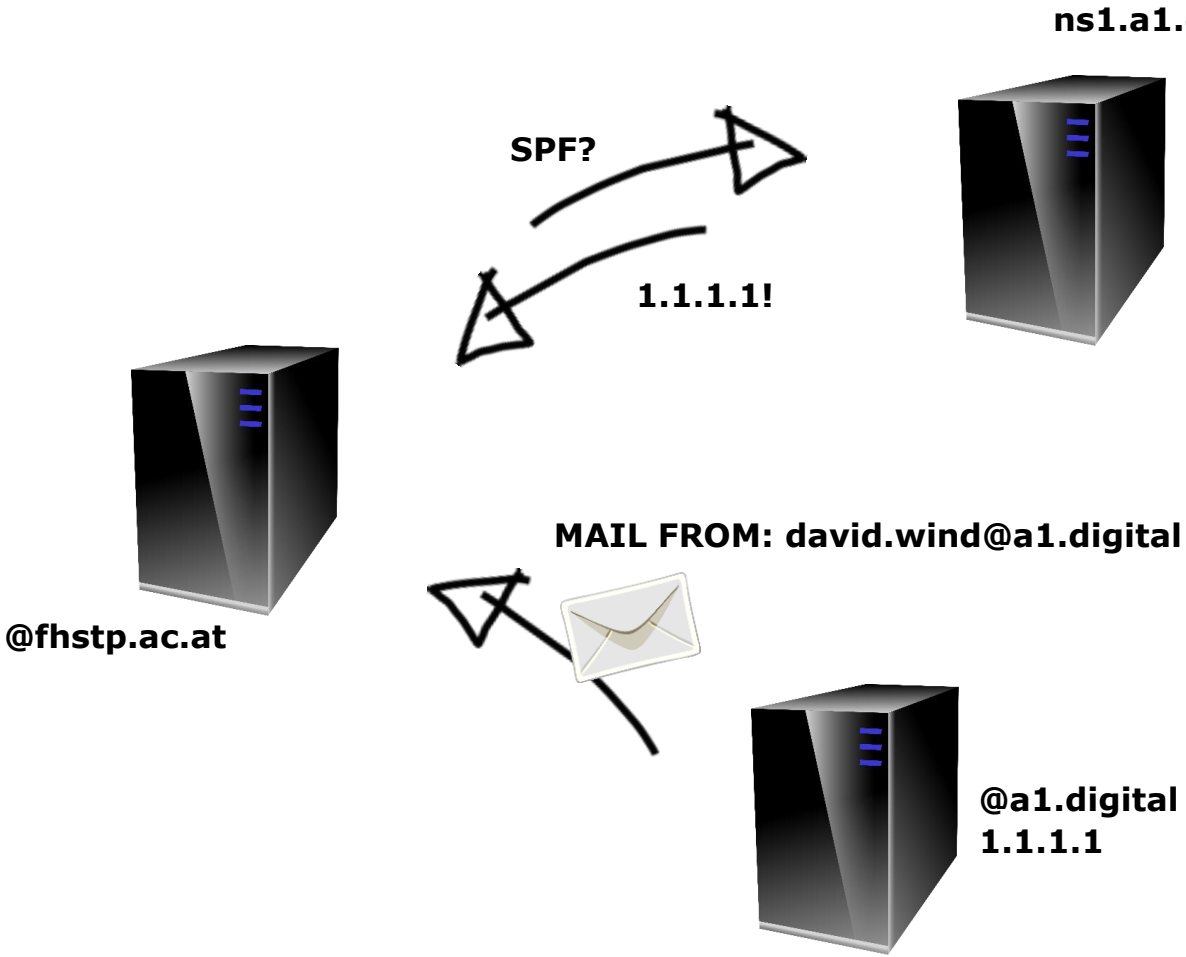
https://umbrella.cisco.com/blog/2016/02/08/grammar-and-spelling-errors-in-phishing-and-malware/



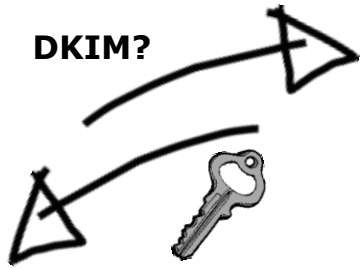
A1 Digital

https://twitter.com/alex_lanstein/status/1192092706396233728

Spoofing Emails


ns1.a1.digital
SPF?
1.1.1.1!
MAIL FROM: david.wind@a1.digital
@fhstp.ac.at
@a1.digital
1.1.1.1

ns1.a1.digital



@fhstp.ac.at

MAIL FROM: david.wind@a1.digital

A1 Digital

Lookalike Domains

mirosoft.com

netlfix.com

micrsoft.com

spakrasse.at

unqia.com

A1 Digital

Punycode

Punycode Domains

- Special encoding to convert Unicode to ASCII
- Firefox still vulnerable by default

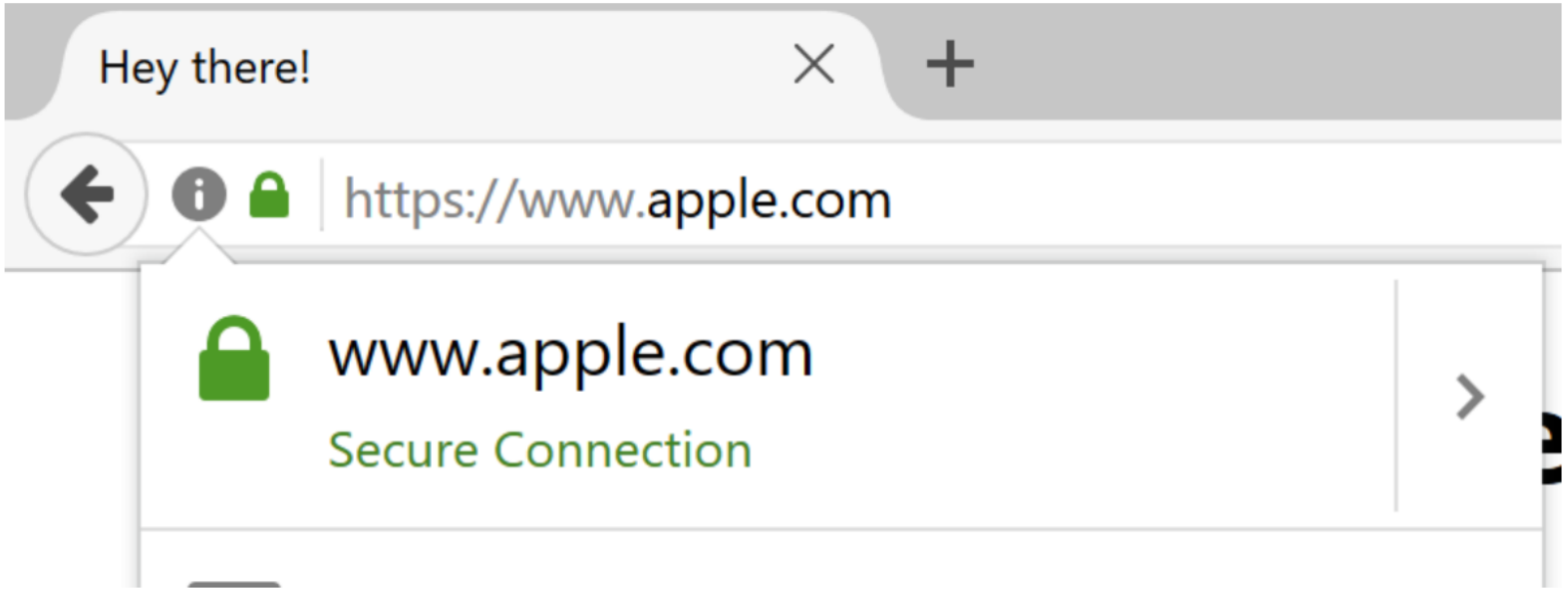
A1 Digital

Phishing with Unicode Domains - X

https://www.xudongz.com/bl

Phishing with Unicode Domains

Posted by Xudong Zheng on April 14, 2017



Before I explain the details of the vulnerability, you should take a look at the proof-of-concept.

Punycode converter

or an IDN converter, a tool for Punycode to Text/Unicode and vice-versa conversion

Text

Example: **點看**

Copy

a1.digital

Convert to Punycode >>

Punycode

Example: **xn--c1yn36f**

Copy

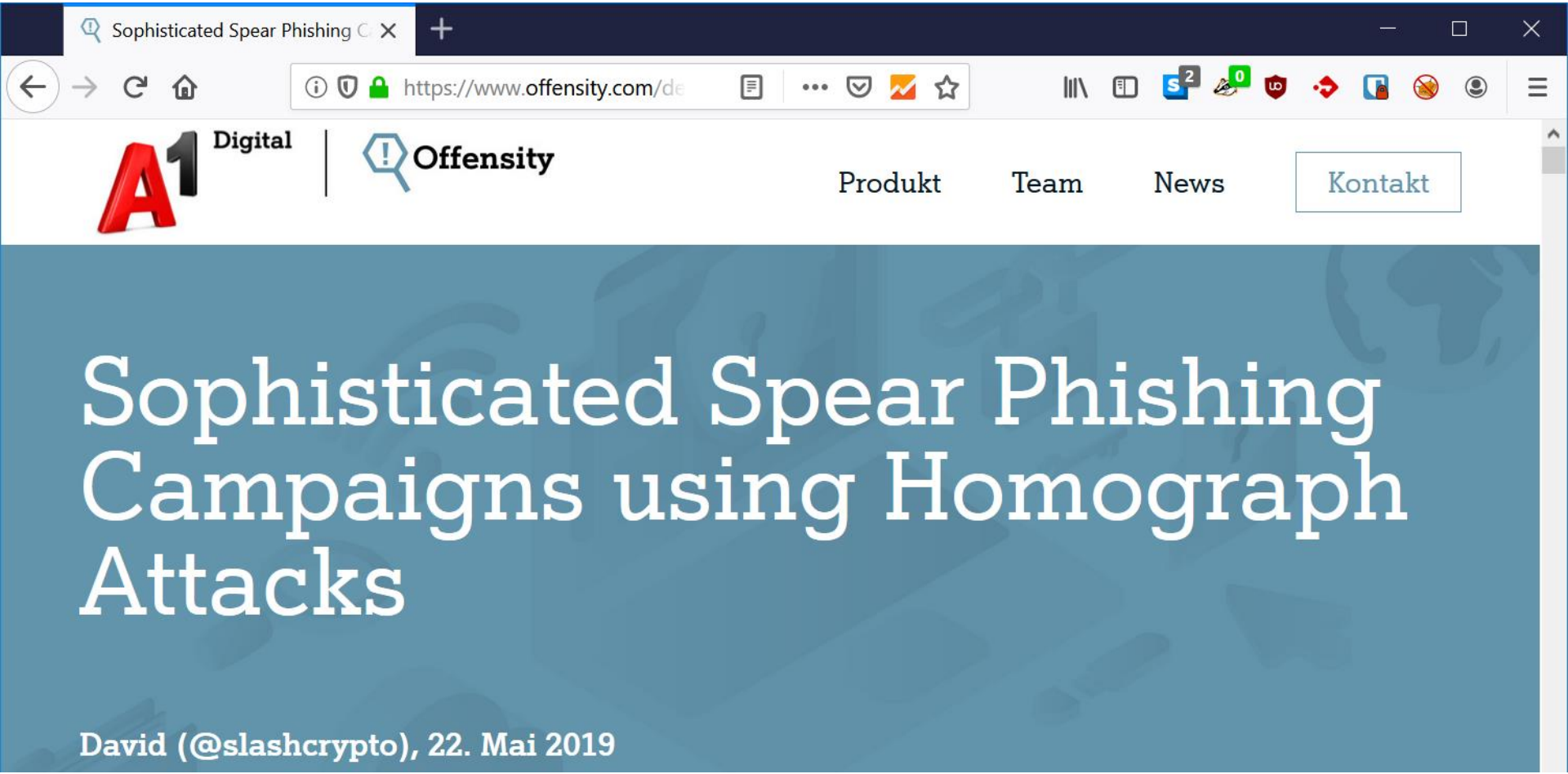
xn--1-7sb.digital

<< Convert to text

https://www.xudongz.com/blog/2017/idn-phishing/

What about Emails ???

A1 Digital



https://www.offensity.com/de/blog/sophisticated-spear-phishing-campaigns-using-homograph-attacks/

Sign Up for our new Security Awareness Course

BS

Bud Spencer <bud.spencer@a1.digital>

To Wind David

Reply | Reply All | Forward | ...

Tue 5/21/2019 3:41 PM

Retention Policy A1 - E-Mail-Policy: Posteingang - Nach 3 Jahren löschen (3 years) Expires 5/25/2022

This email has been sent from an international address and contains characters from multiple languages that may look alike. Click here to learn more.

Sign Up for our new Security Awareness Course

BS

Bud Spencer <bud.spencer@a1.digital>

To Wind David

Retention Policy A1 - E-Mail-Policy: Posteingang - Nach 3 J Expires 5/25/2022

This email has been sent from an international address and contains characters from mul alike. Click here to learn more.

Hello Ter

You can fi

https://a1

Kind Rega

Bud

--

Bud Spen

Security

Professional Services

A1 Digital International GmbH
Lassallestraße 9 1020 Wien
M +43 664 66 12345
F +43 50 664 9 54321
@ bud.spencer@a1.digital

Reply Reply All Forward

BS

Bud Spencer <bud.spencer@a1.digital> terence.hill@offensity.com

Sign Up for our new Security Awareness Course

Hello Terence,

You can find the registration link for our security awareness training below:
https://a1.digital/security-awareness-training

Kind Regards
Bud

--
Bud Spencer
Security
Professional Services

A1 Digital

Discard Pop Out

Send

To bud.spencer@a1.digital

Cc

Subject RE: Sign Up for our new Security Awareness Course

Great!

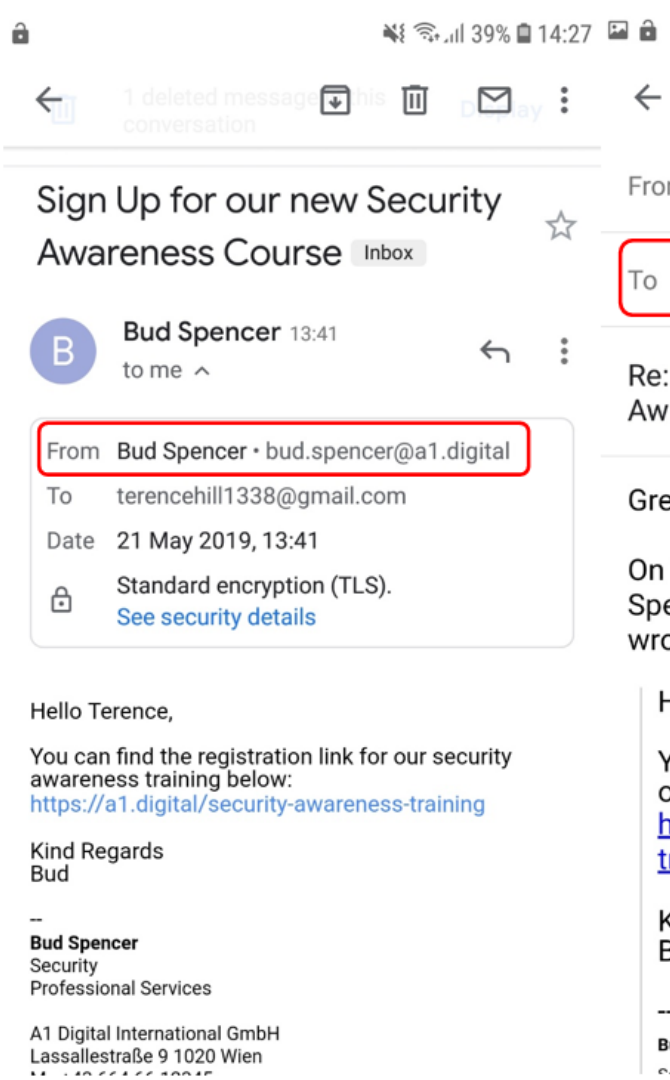
From: Bud Spencer <bud.spencer@a1.digital>
Sent: Tuesday, May 21, 2019 3:41 PM
To: Wind David <David.Wind@a1.digital>
Subject: Sign Up for our new Security Awareness Course

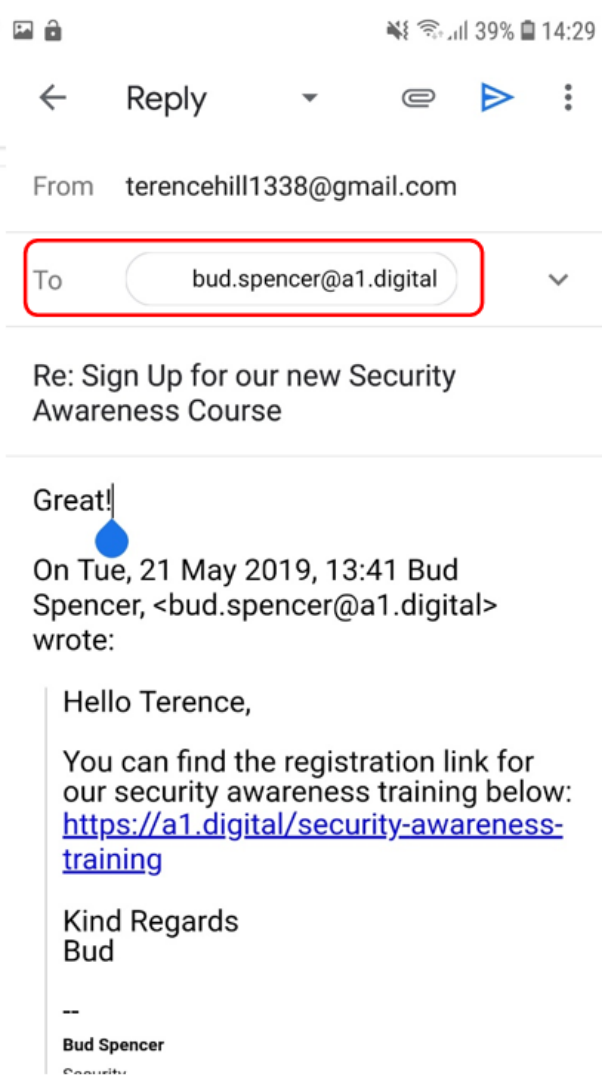
Hello Terence,

You can find the registration link for our security awareness training below:
https://a1.digital/security-awareness-training

Kind Regards
Bud

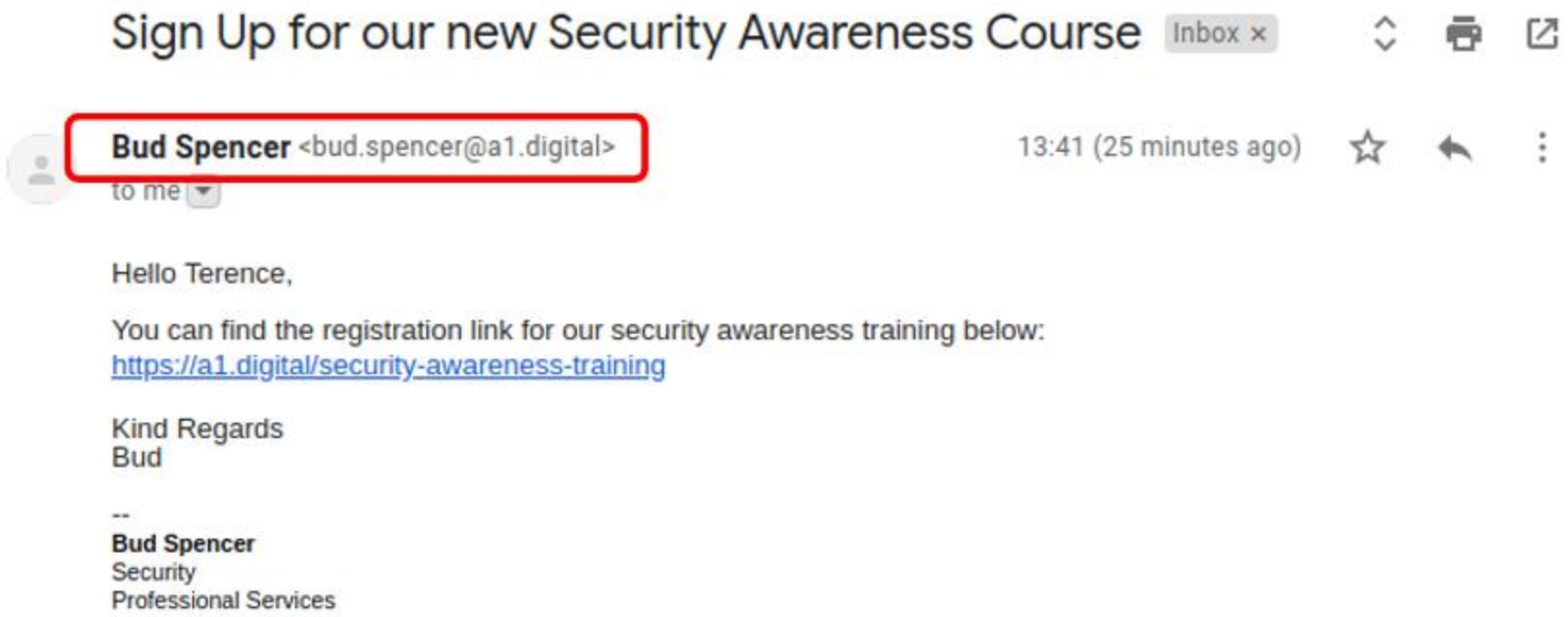
Gmail Android





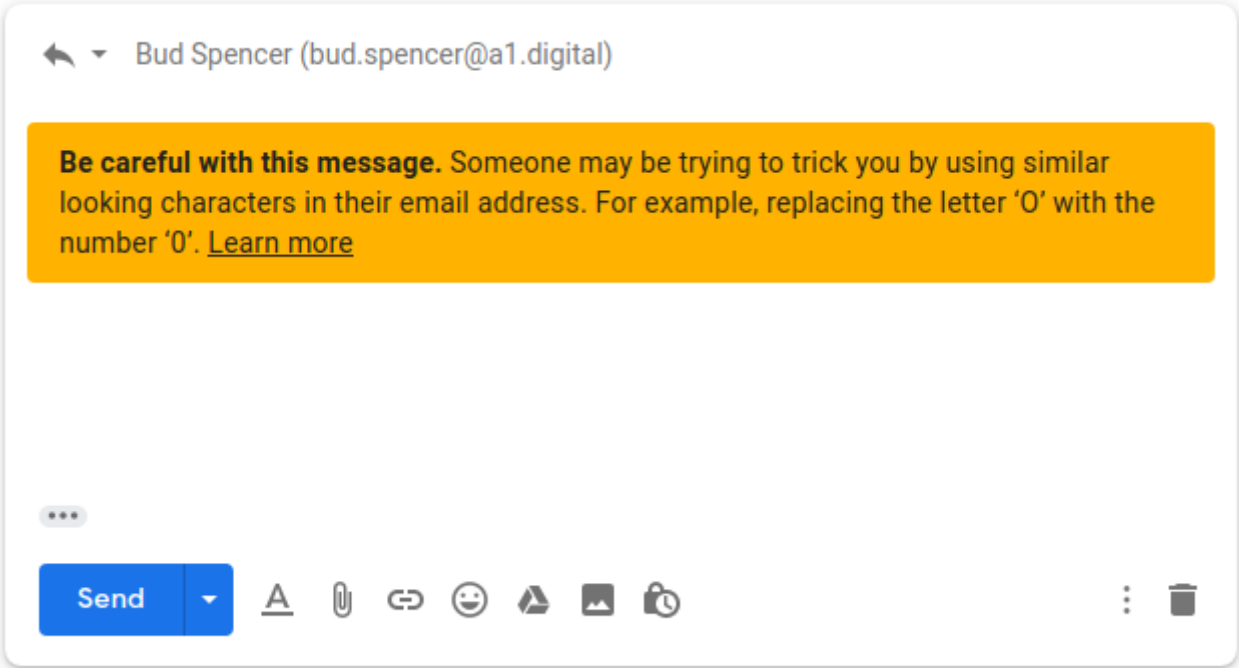
A1 Digital

Gmail Web



A1 Digital

Gmail Web


Bud Spencer (bud.spencer@a1.digital)
Be careful with this message. Someone may be trying to trick you by using similar looking characters in their email address. For example, replacing the letter 'O' with the number '0'. Learn more
Send

Outlook Web

Sign Up for our new Security Awareness Course

Label: A1 - E-Mail-Policy: Posteingang - Nach 6 Monaten löschen (6 months) Expires: Sun 17 Nov 2019 14:16

BS

Bud Spencer <bud.spencer@a1.digital>

Di, 21.05.2019 15:16

Hello Terence,

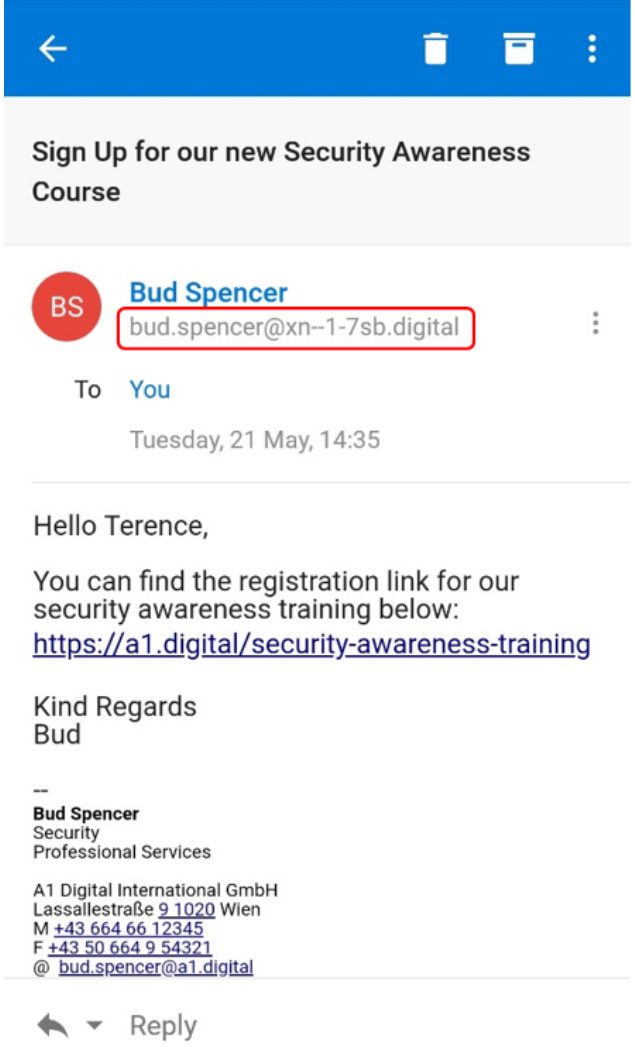
You can find the registration link for our security awareness training below:
https://a1.digital/security-awareness-training

Kind Regards
Bud

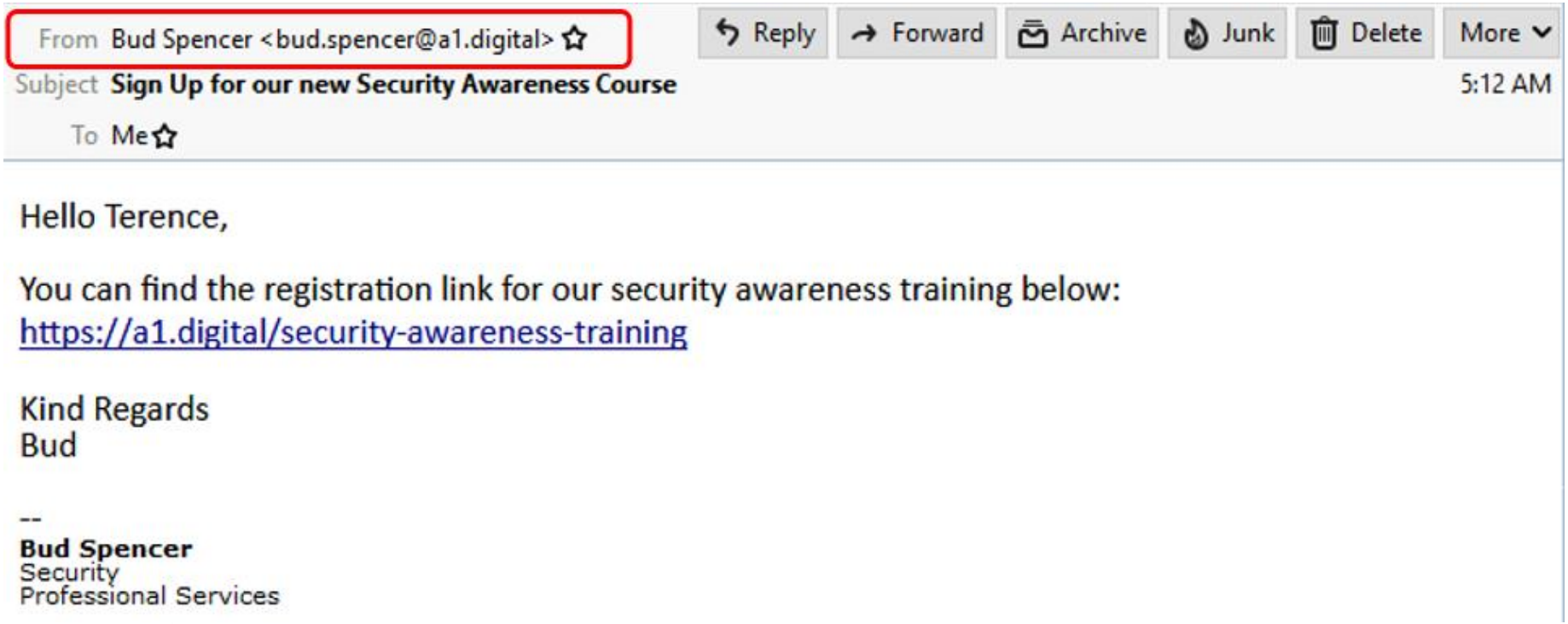
--
Bud Spencer
Security
Professional Services

A1 Digital

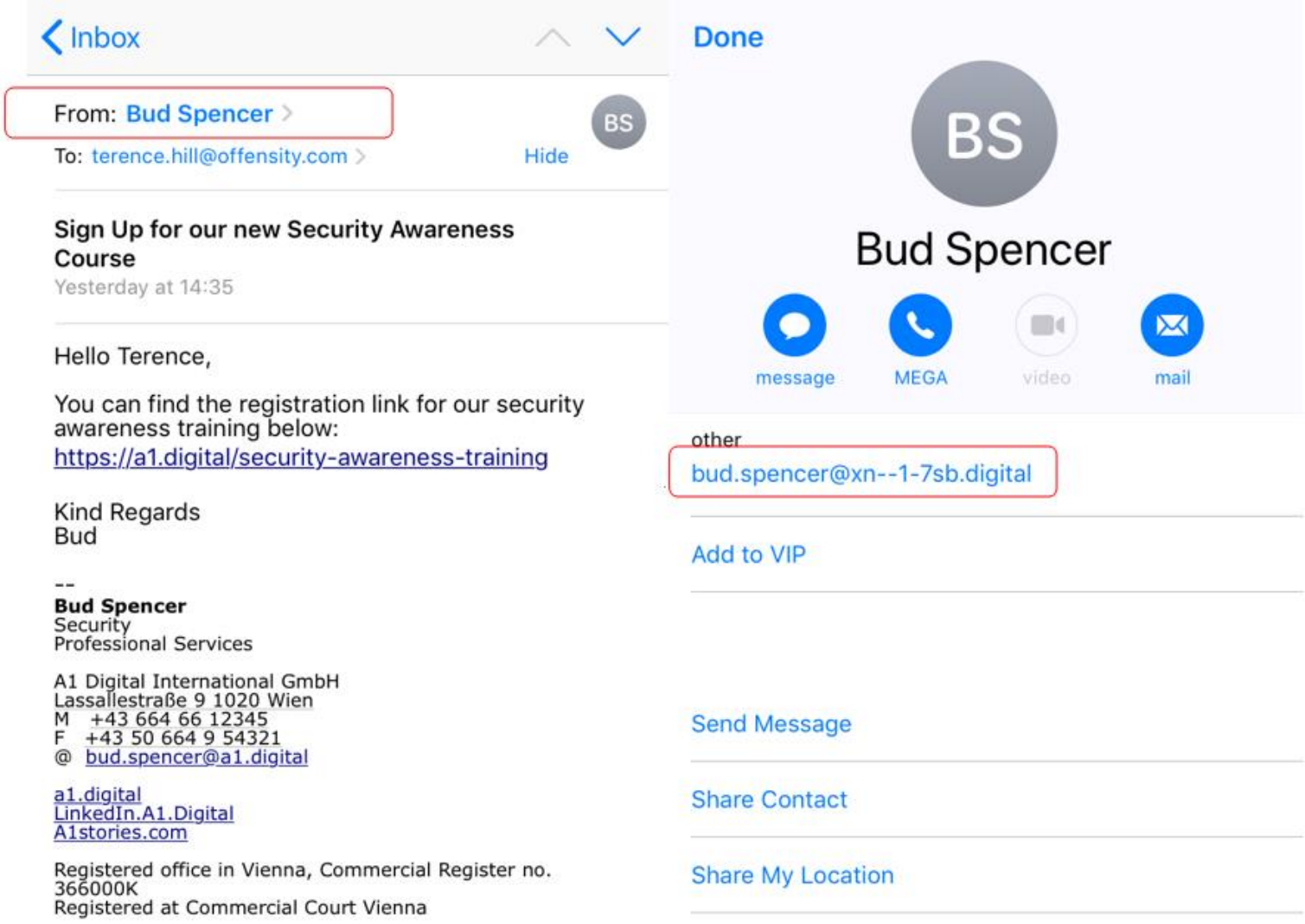
Outlook Android



Thunderbird



Apple



Inbox

From: Bud Spencer

To: terence.hill@offensity.com Hide

BS

Sign Up for our new Security Awareness Course

Yesterday at 14:35

Hello Terence,

You can find the registration link for our security awareness training below:
https://a1.digital/security-awareness-training

Kind Regards
Bud

--
Bud Spencer
Security
Professional Services

A1 Digital International GmbH
Lassallestraße 9 1020 Wien
M +43 664 66 12345
F +43 50 664 9 54321
@ bud.spencer@a1.digital

a1.digital
LinkedIn.A1.Digital
A1stories.com

Registered office in Vienna, Commercial Register no. 366000K
Registered at Commercial Court Vienna

Done

BS

Bud Spencer

message MEGA video mail

other

bud.spencer@xn--1-7sb.digital

Add to VIP

Send Message

Share Contact

Share My Location

A1 Digital

Overview

	Detectable when reading Mail	Detectable when replying to Mail
Outlook for Windows	NO	NO
Outlook for Mobile	YES	YES
Office365 Web	NO	NO
Gmail Web	NO	YES
Gmail Android	NO	NO
IMail (Mobile)	YES	YES
Thunderbird	NO	NO

A1 Digital

Phishing Websites

README.md

..Modlishka..

Modlishka is a powerful and flexible HTTP reverse proxy. It implements an entirely new and interesting approach of handling browser-based HTTP traffic flow, which allows to transparently proxy multi-domain destination traffic, both TLS and non-TLS, over a single domain, without a requirement of installing any additional certificate on the client. What does this exactly mean? In short, it simply has a lot of potential, that can be used in many use case scenarios...

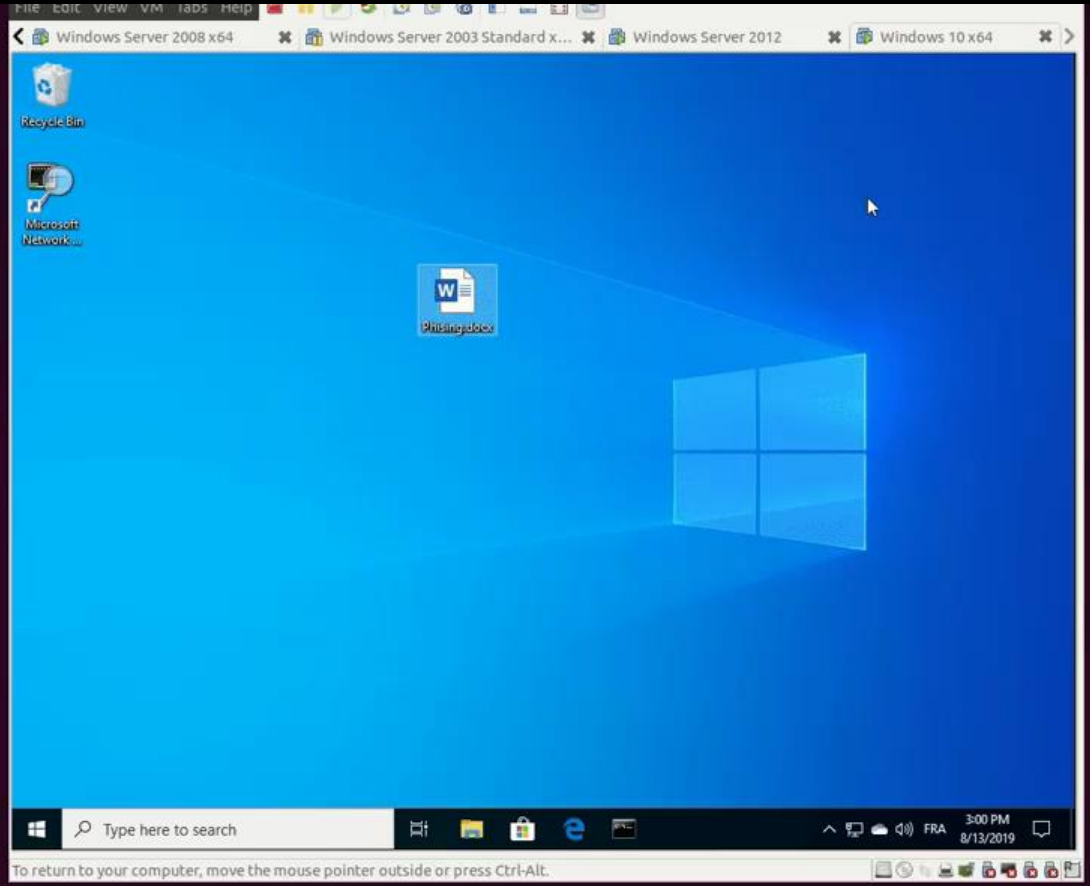
A1 Digital

https://github.com/drk1wi/Modlishka

What else …?

Collecting NTLMv1/v2 (Net-NTLM) Hashes

```
NBT-NS, LLMNR & MDNS Responder 2.3.3.9

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [ON]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [OFF]

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [178.13.32.55]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']


[!] Error starting UDP server on port 5355, check permissions or other servers running.
[!] Error starting UDP server on port 5353, check permissions or other servers running.
[+] Listening for events...
```



Digital

Questions?