Email Trust Issues?

Find out what you can do to help

Email Trust Issues?

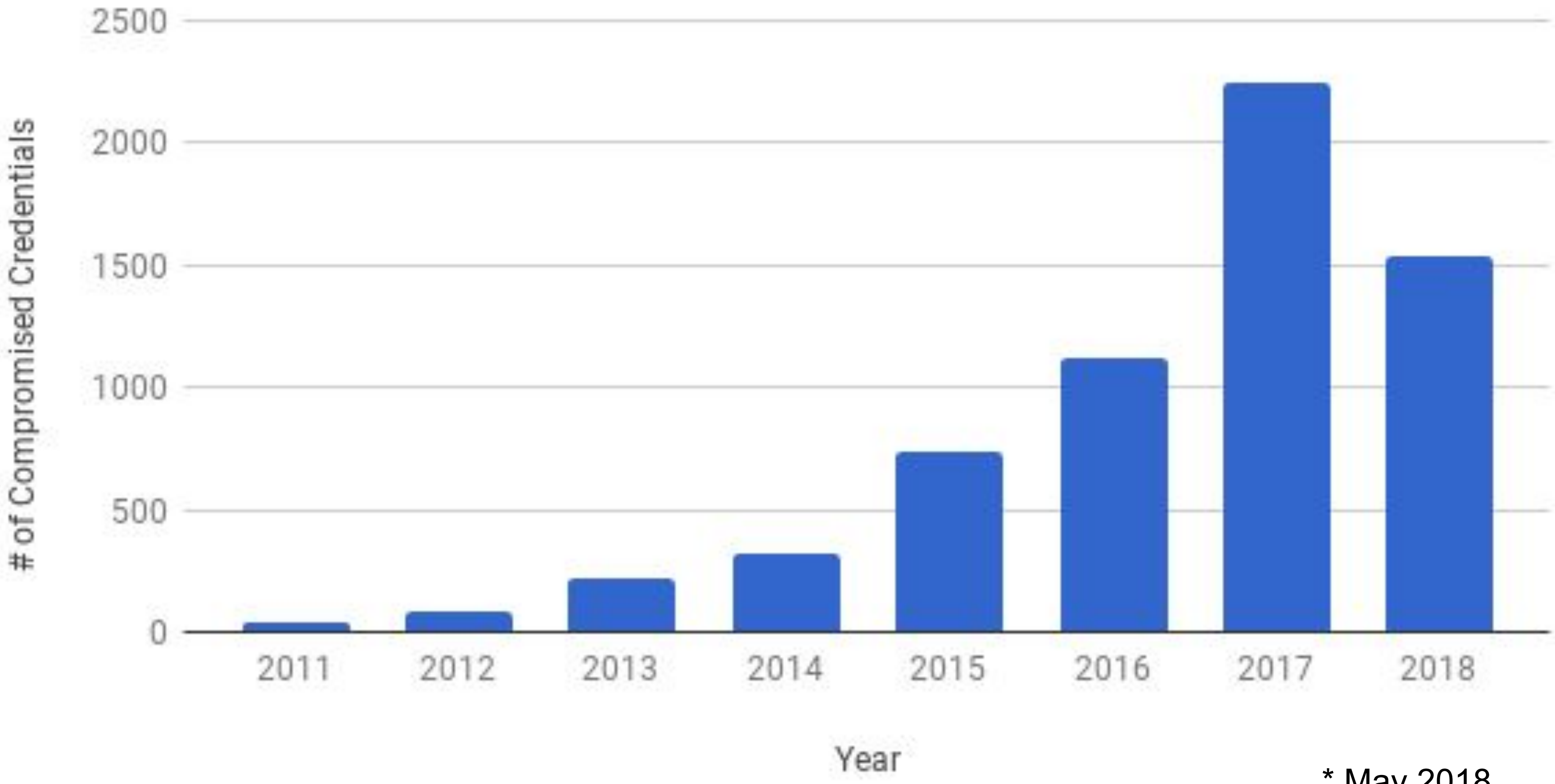
Key Concepts:

A. What UW-Madison is doing to improve email security
B. How IT Professionals can help make email more secure

Problem Areas of Focus:

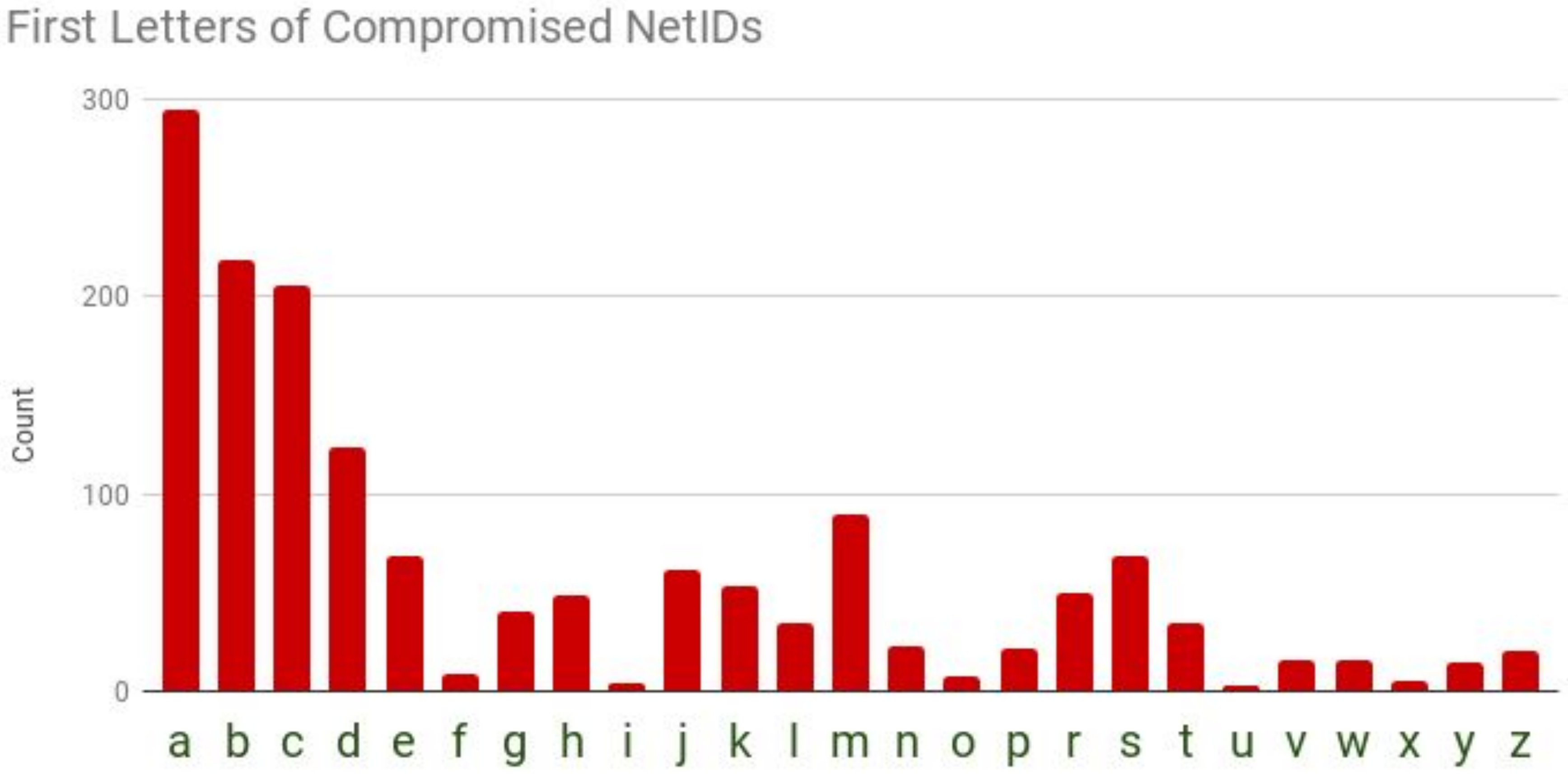
1. ***Attacks*** - Credentials are stolen and the email service is under constant attack.
2. ***Authenticity*** - Domains are being spoofed and that undermines the trust in our email.

Compromised Credentials Caught Abusing UW-Madison Email Services

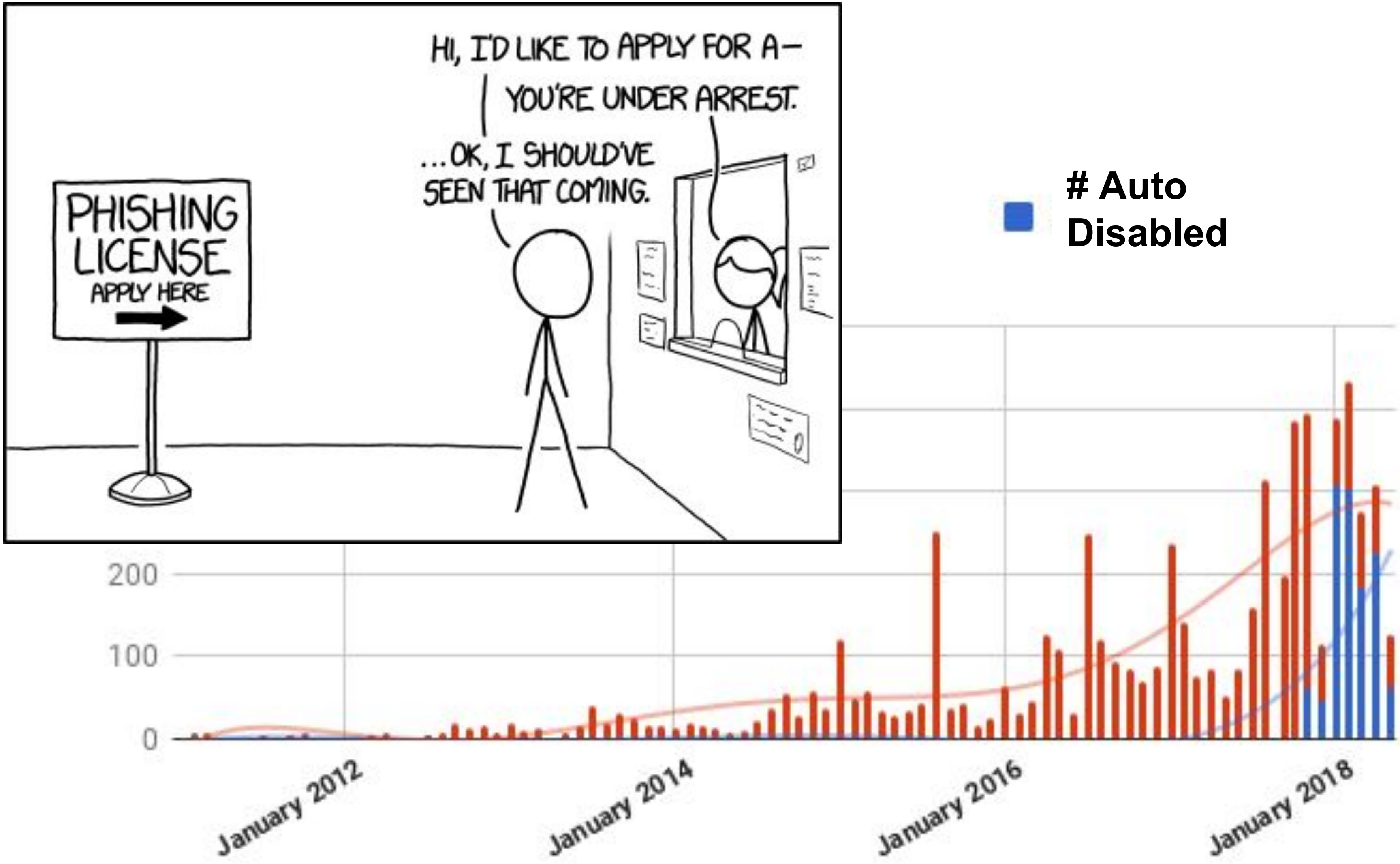


* May 2018

Attackers Are Human
Humans Leave Patterns



Attacks - Automated Mitigation



Attacks - What can people do?

Multi-Factor Auth

→ Assume your password is already compromised

Password Manager

→ Use unique passwords
& never type into web pages

DMARC

→ Build trust in email
& help stop email spoofing

Email Authentication

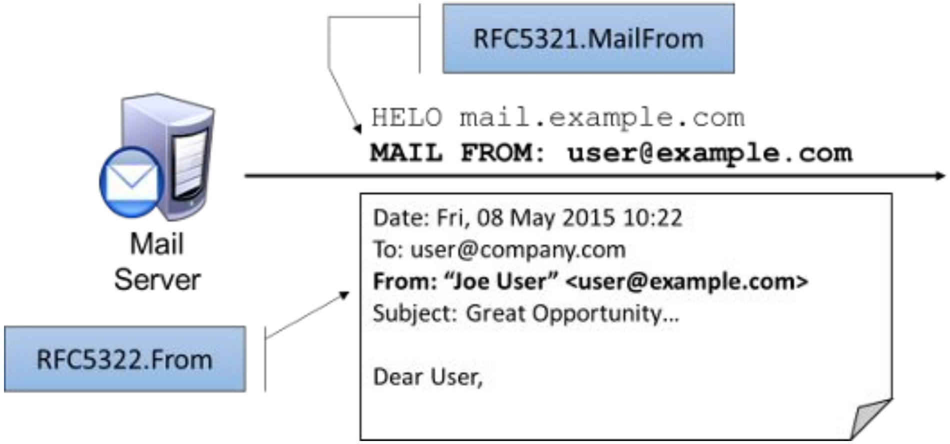
go.wisc.edu/email-authenticity

DMARC -

Domain-based Message Authentication, Reporting & Conformance

DMARC protects the domain in the “From:” which users can see

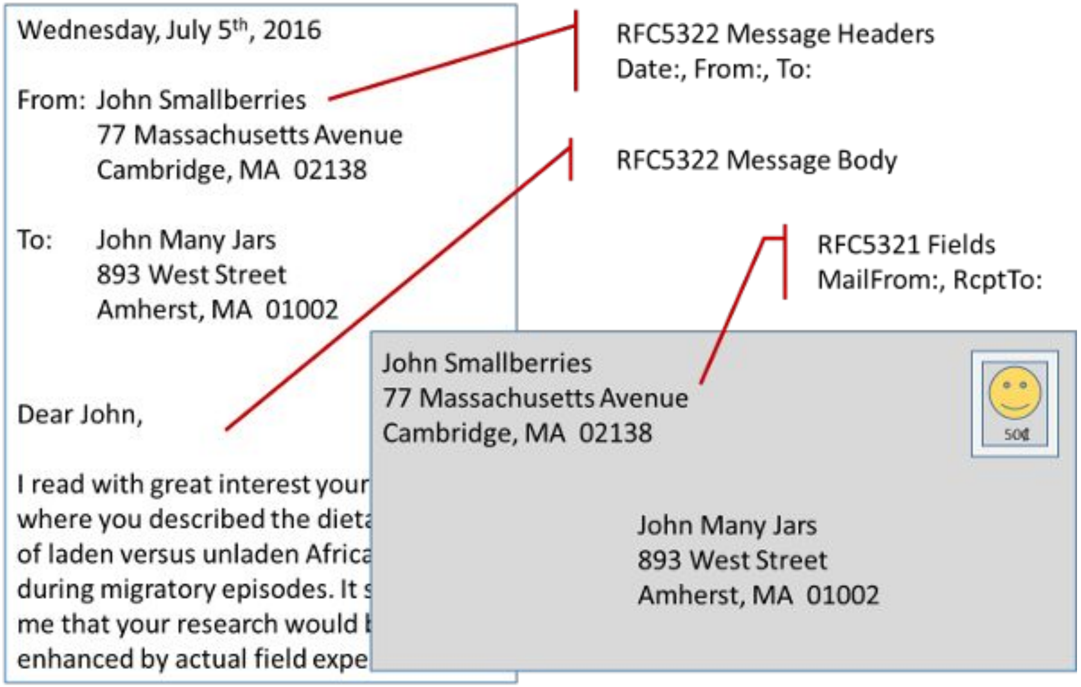
dmarc.org



```
HELO mail.example.com
MAIL FROM: user@example.com
```

Date: Fri, 08 May 2015 10:22
To: user@company.com
From: “Joe User” <user@example.com>
Subject: Great Opportunity…

Dear User,



Wednesday, July 5th, 2016

From: John Smallberries
77 Massachusetts Avenue
Cambridge, MA 02138

To: John Many Jars
893 West Street
Amherst, MA 01002

Dear John,

I read with great interest your
where you described the dieta
of laden versus unladen Africa
during migratory episodes. It s
me that your research would b
enhanced by actual field expe

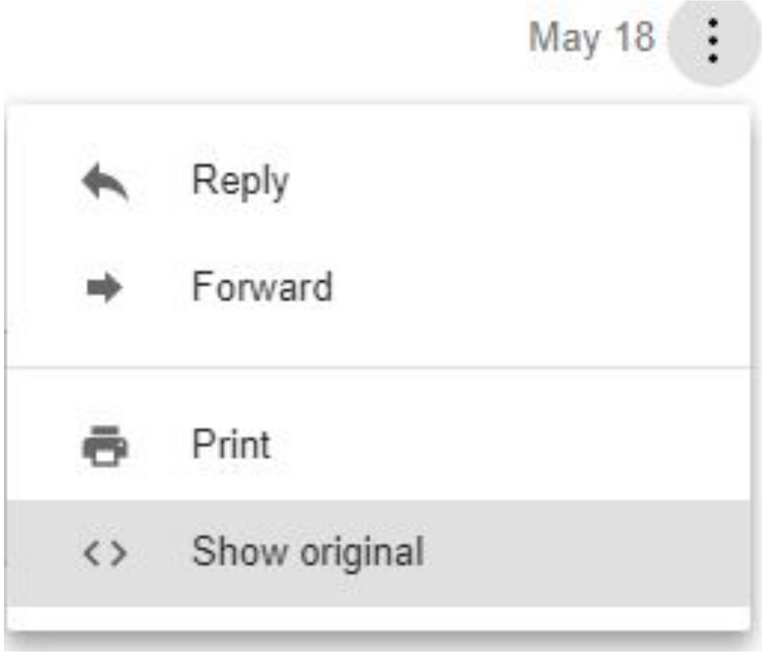
John Smallberries
77 Massachusetts Avenue
Cambridge, MA 02138

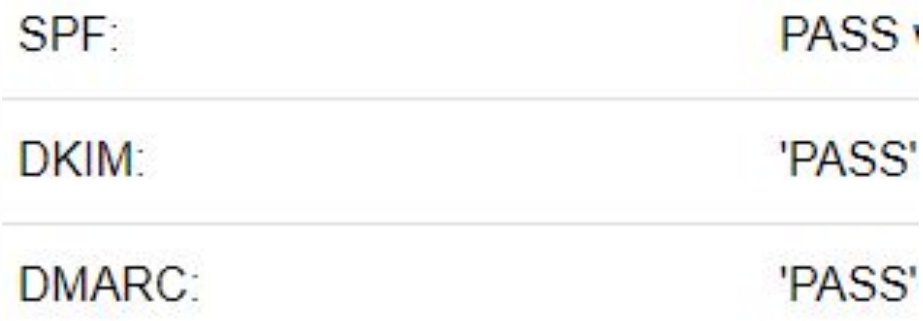
John Many Jars
893 West Street
Amherst, MA 01002

SPF

DKIM.org

Testing DMARC Is Easy - Just Send A Message to Gmail





SPF:	PASS
DKIM:	'PASS'
DMARC:	'PASS'

Authentication-Results:

dkim=pass
spf=pass
smtp.mailfrom=...@***dept.wisc.edu***
dmarc=pass
header.from=***dept.wisc.edu***

Enhancing Email Authenticity at UW

Today	**Future**
Too many email senders spoof wisc.edu	Publish a secure DMARC policy for wisc.edu
Lots of sub domains aren't protected	Help subdomain owners to adopt DMARC

Systems that can’t authorize the user to their own address can’t use @wisc.edu

Don't	**Do**
Don't use @wisc.edu	Use @subdomain.wisc.edu
Don't spoof the From header to “prevent replies”	Ensure the From header matches the SMTP From
Don't spoof any domain (even your own)	Ensure your messages pass DMARC with SPF or DKIM

DMARC Challenges

Mailing lists and forwarding → Need to rewrite the From header

https://kb.wisc.edu/81107

DNS lookup limit for SPF → Requires more subdomains

https://tools.wordtothewise.com/spf/check/uwosh.edu

Inbound enforcement → Rewrite or block inbound messages

dmarc-test@g-groups.wisc.edu

Vendors don’t really understand DKIM or domain alignment and assume spoofing is OK

Other things to think about

Take an adversarial perspective to messages you send

How do users know your message isn’t a threat?

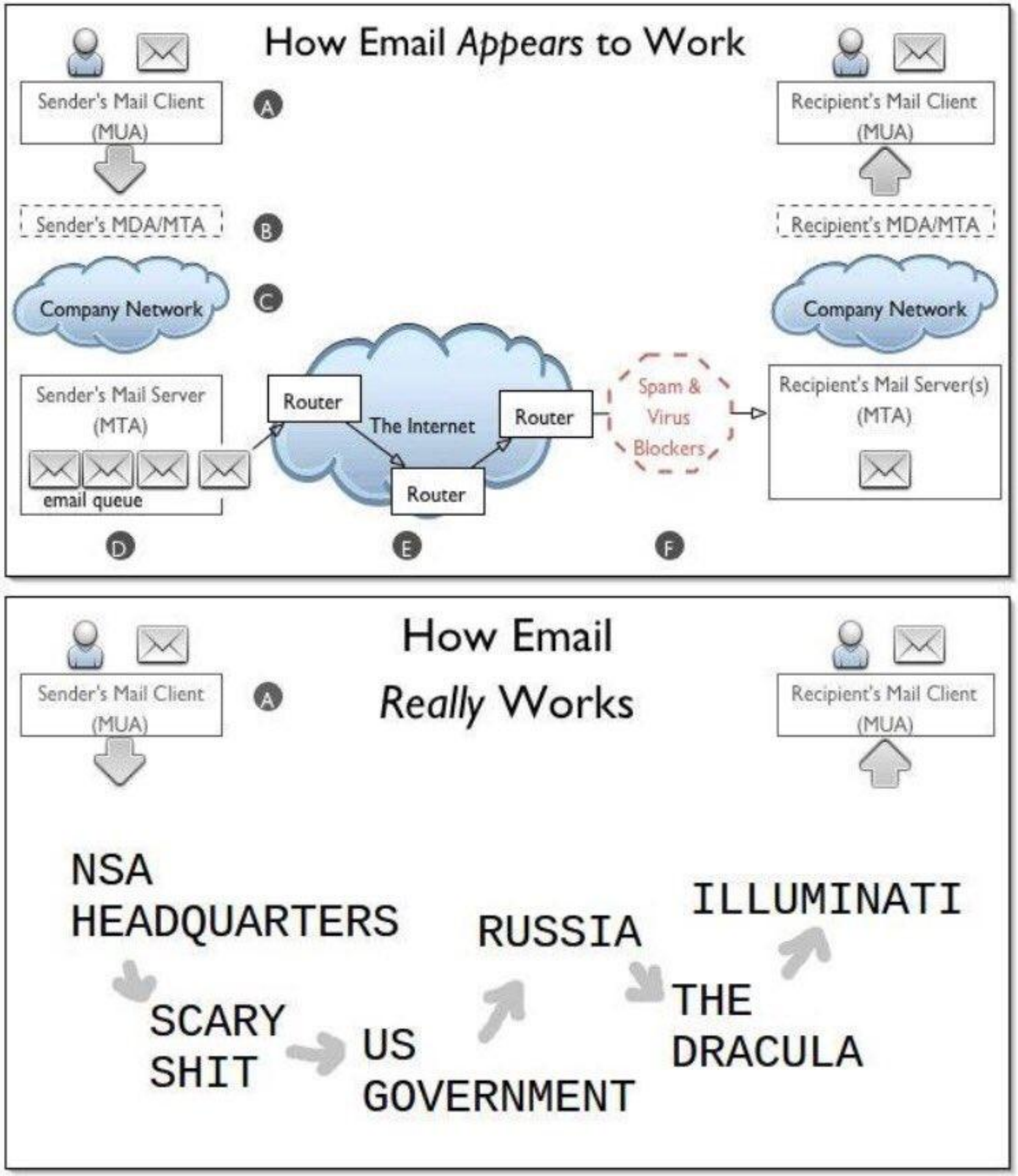
Is email even necessary for your application?

Can email content be mirrored to the web so IT staff can verify?

Link to a website for your subdomain (WiscWeb, Google Sites)

Questions?

jesse.thompson@wisc.edu


How Email *Appears* to Work
Sender's Mail Client (MUA)
A
Sender's MDA/MTA
B
Company Network
C
Sender's Mail Server (MTA)
email queue
D
Router
The Internet
Router
Router
E
Spam & Virus Blockers
F
Recipient's Mail Client (MUA)
Recipient's MDA/MTA
Company Network
Recipient's Mail Server(s) (MTA)
How Email *Really* Works
Sender's Mail Client (MUA)
A
Recipient's Mail Client (MUA)
NSA HEADQUARTERS
SCARY SHIT
US GOVERNMENT
RUSSIA
THE DRACULA
ILLUMINATI