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

First Letters of Compromised NetIDs
Attacks - Automated Mitigation
Attacks - What can people do?

- **Password Manager**
  → Use unique passwords & never type into web pages

- **Multi-Factor Auth**
  → Assume your password is already compromised

- **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

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 paper where you described the dietary habits of laden versus unladen African migratory birds during migratory episodes. It seems to me that your research would be greatly enhanced by actual field experience.

DKIM.org

RFC5321 Message Headers
Date:, From:, To:

RFC5322 Message Body

RFC5321 Fields
MailFrom:, RcpTo:
Testing DMARC Is Easy - Just Send A Message to Gmail

Authentication-Results:
dkim=pass
spf=pass
smtp.mailfrom=...@dept.wisc.edu
dmarc=pass
header.from=dept.wisc.edu
Enhancing Email Authenticity at UW

**Today**
- Too many email senders spoof wisc.edu
- Lots of sub domains aren't protected

**Future**
- Publish a secure DMARC policy for wisc.edu
- Help subdomain owners to adopt DMARC
Systems that can’t authorize the user to their own address can’t use @wisc.edu

**Don't**

- Don't use @wisc.edu
- Don't spoof the From header to “prevent replies”
- Don't spoof any domain (even your own)

**Do**

- Use @subdomain.wisc.edu
- Ensure the From header matches the SMTP From
- 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