SUMIT

IT SECURITY EVENT SERIES

WEEKLY IN OCTOBER

Reimagined

INFORMATION AND TECHNOLOGY SERVICES
UNIVERSITY OF MICHIGAN

Follow Along @umichTECH
Join the Coversation #SUMIT21

Two Capabilities, One Goal: Email Security with Area 1 and Virtru

Dennis Neil and Brian Cors

Information Assurance and
ITS Support Services

INFORMATION AND
TECHNOLOGY SERVICES
UNIVERSITY OF MICHIGAN

SUMIT Reimagined

The Current Threat Landscape

Phishing, or the practice of sending someone a fake or spoofed message in order to get them to reveal sensitive information or to install malicious software, continues to be a threat, and more specifically a source of ransomware infections. Malware taking advantage of phishing can lead to:

- Loss or corruption of data
- Reputational and financial harm
- Legal and/or regulatory issues

What is Area 1?

- A cloud-based anti-phishing solution
- It works with the U-M Gmail system to detect and mitigate threats in email
- Is customized to meet our needs
- Used across U-M, including by Michigan Medicine

Complements Existing Capabilities

- Area 1 crawls the internet identifying the websites, tools, and techniques used by attackers
- It uses those characteristics to calculate the risk of messages
- It flags malicious messages so that they are delivered to a user's spam folder
- By automating anti-phishing, it frees up security staff to focus on work that requires their expertise

What Is the Goal of a Phish?

Often driven by a false sense of urgency or with the intent to provide immediate benefit, the intended actions in a phish include:

- Updating a password
- Promise of personal financial benefit
- Verifying an online account

What Does Area 1 Look For?

Area 1 works by identifying specific, high-risk characteristics of email which include:

- **Domain spoof:** Appears to originate from U-M
- **Name spoof:** Poses as a U-M trusted and known individual
- **Attributes spoof:** Provides copycat logos or branding
- **Known attack sources:** Existing threat actors and campaigns

Area 1 Anti-Phishing

Area 1 Can’t Do it Alone

Since the roll out in March, Area 1 has processed 700M+ messages and mitigated 700K+ malicious messages

Area1 is just part of an overall strategy. Keeping systems and data secure includes a comprehensive set of steps including:

- **Using two-factor authentication whenever possible**
- **Keeping hardware and software up-to-date**
- **Backing up data and managing remote access**

What Can *I* do to Protect My Email?

What is Virtru?

- An easy to use, email security enhancement tool for Gmail
- Simplifies end-to-end email encryption
- Is **available at no cost** to all Google at U-M Gmail users *(U-M Faculty, Staff, and Students using Gmail)*

NOTE: *Michigan Medicine email users can use the encryption tool already provided by Michigan Medicine.*

What Virtru Does

- Encrypt email and attachments
- Prevent email content from being opened when forwarded
- Watermark attachments sent to recipients
- Set an email expiry date
- Revoke access to previously sent messages on demand
- Non-Virtru users can read and reply to messages you send them

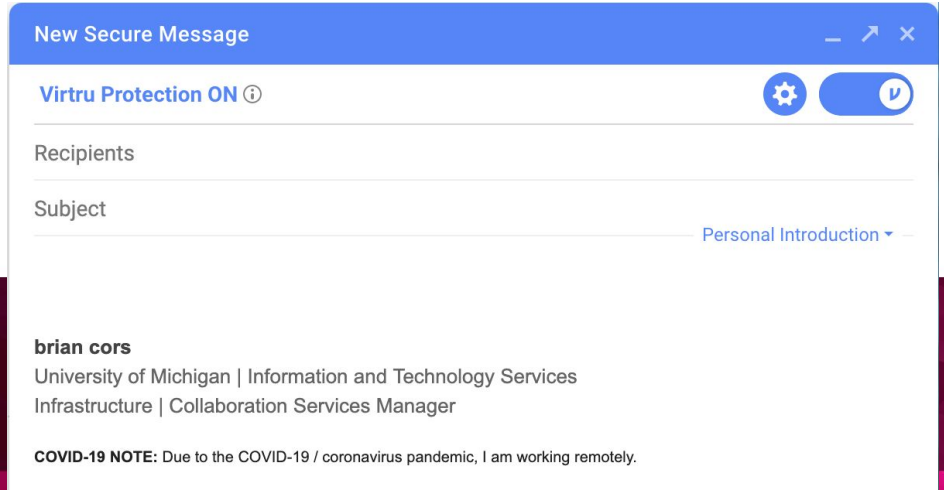
Getting Started with Virtru

In order to use Virtru:

- Currently need to use Google Chrome and the Gmail web interface
- Install the Virtru Email Protection Google Chrome extension
- A free iOS or Android application is available for mobile devices *(NOTE: Not recommended as primary email app)*

Start Using Virtru!

Let’s get you started using Virtru. **Right now.**



INFORMATION AND TECHNOLOGY SERVICES
UNIVERSITY OF MICHIGAN

Use Cases

Use Virtru to encrypt your messages and control access to them. For example, encrypt emails that include:

- Personally identifiable information (PII), such as name, birth date, or address
- Excel spreadsheet attachment with U-M names and uniqnames or UMID numbers
- Grades and other student education records
- Approved for Export Controlled data*

Use Cases to Avoid

Some types of sensitive information **should not be sent via email**, even with Virtru encryption. For example, do not send email with:

- Payment Card Industry (PCI) data (credit cards)
- Certain types of regulated data, such as Federal Information Security Act (FISMA) data

Visit the U-M Sensitive Data Guide to understand what Virtru can be used for.

Things to Know

- Subject lines of email message are never encrypted
- Vitru available via Google Chrome and the Virtru extension
- Virtru will work with MCommunity groups
- Gmail may try to auto-translate decrypted messages
- You will periodically be asked to re-activate Virtru

NOTE: *MCommunity group sync currently happens at 2:00 EDT / 1:00 EST AM daily.*

Resources and Documentation

Sensitive Data Guide

- Virtru at U-M

Safe Computing

- Virtru: Added Security for Your GMail
- Phishing & Suspicious Email

Questions or Feedback?

Have questions or feedback?

Contact the ITS Service Center

https://its.umich.edu/help