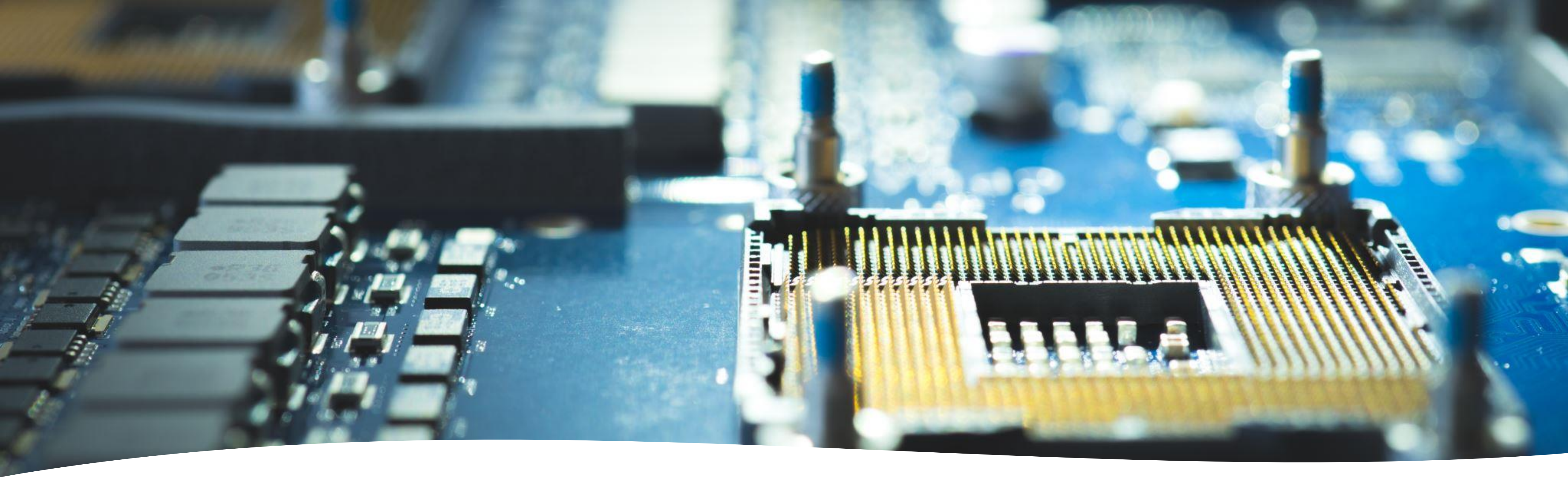


Digital Forensics

Lecture 01- Introduction

Dr. Zunera Jalil

Email: zunera.jalil@au.edu.pk

11th Feb 2025

Course Info

Course Code:	CY- 334
Hours:	02 Theory, 03 Lab
Course Title:	Digital Forensics
Theory Instructor:	Dr. Zunera Jalil
Lab Instructor:	Ms. Memoona Sadaf
Class Time:	Every Monday 10:40 AM-12:30 PM
Google Classroom:	**ge6pddu**

Assessment Plan (Tentative)

Assessment Type	Count	Weightage
Quizes	5	10%
Home Assignments	4	10%
In-Class Assignments	4	
Project	1	10%
Mid semester Exam	1	25%
Final Exam	1	45%

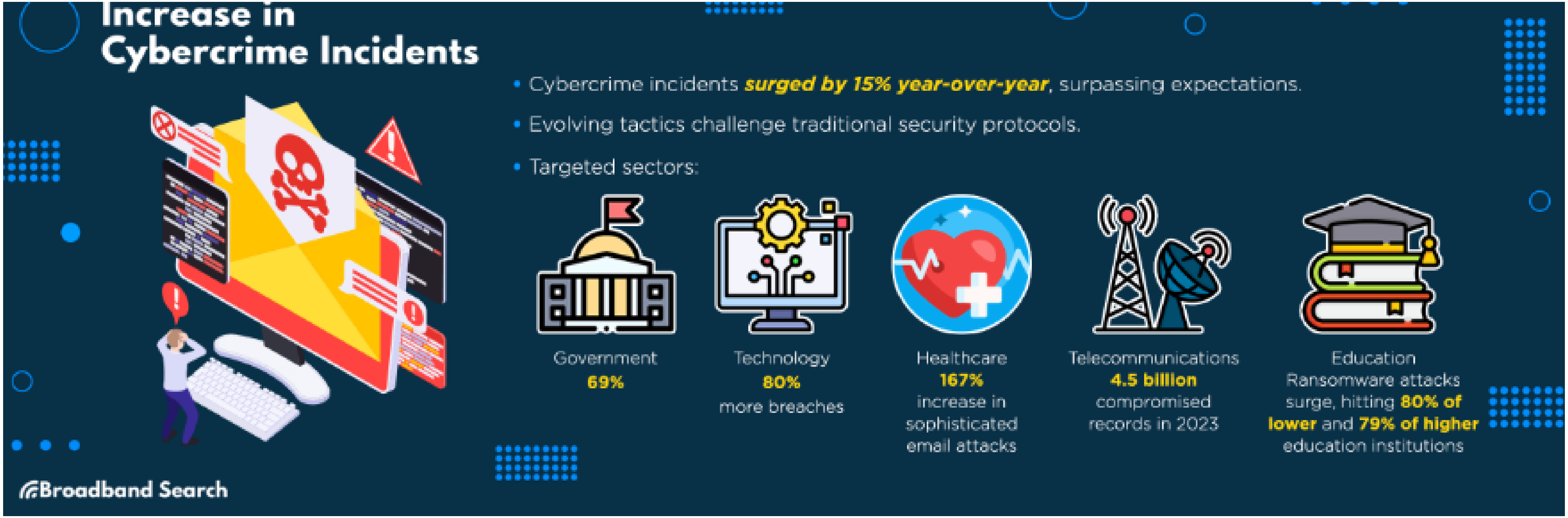
Cybercrime

Cybercrime is criminal activity that either **targets or uses** a computer, a computer network or a networked device.

[Kaspersky]

Cyber crimes

- Phishing Attack
- **Ransomware attack**
- Identity fraud-misusing personal information
- Theft of financial or card payment data.
- Theft and sale of corporate data.
- Harassment
- Spreading hate and inciting terrorism
- Distributing child pornography
- Publishing Derogatory Materials
- E-Money Laundering and Taxation
- ……



Increase in Cybercrime Incidents

- Cybercrime incidents ***surged by 15% year-over-year***, surpassing expectations.
- Evolving tactics challenge traditional security protocols.
- Targeted sectors:

Government
69%

Technology
80%
more breaches

Healthcare
167%
increase in sophisticated email attacks

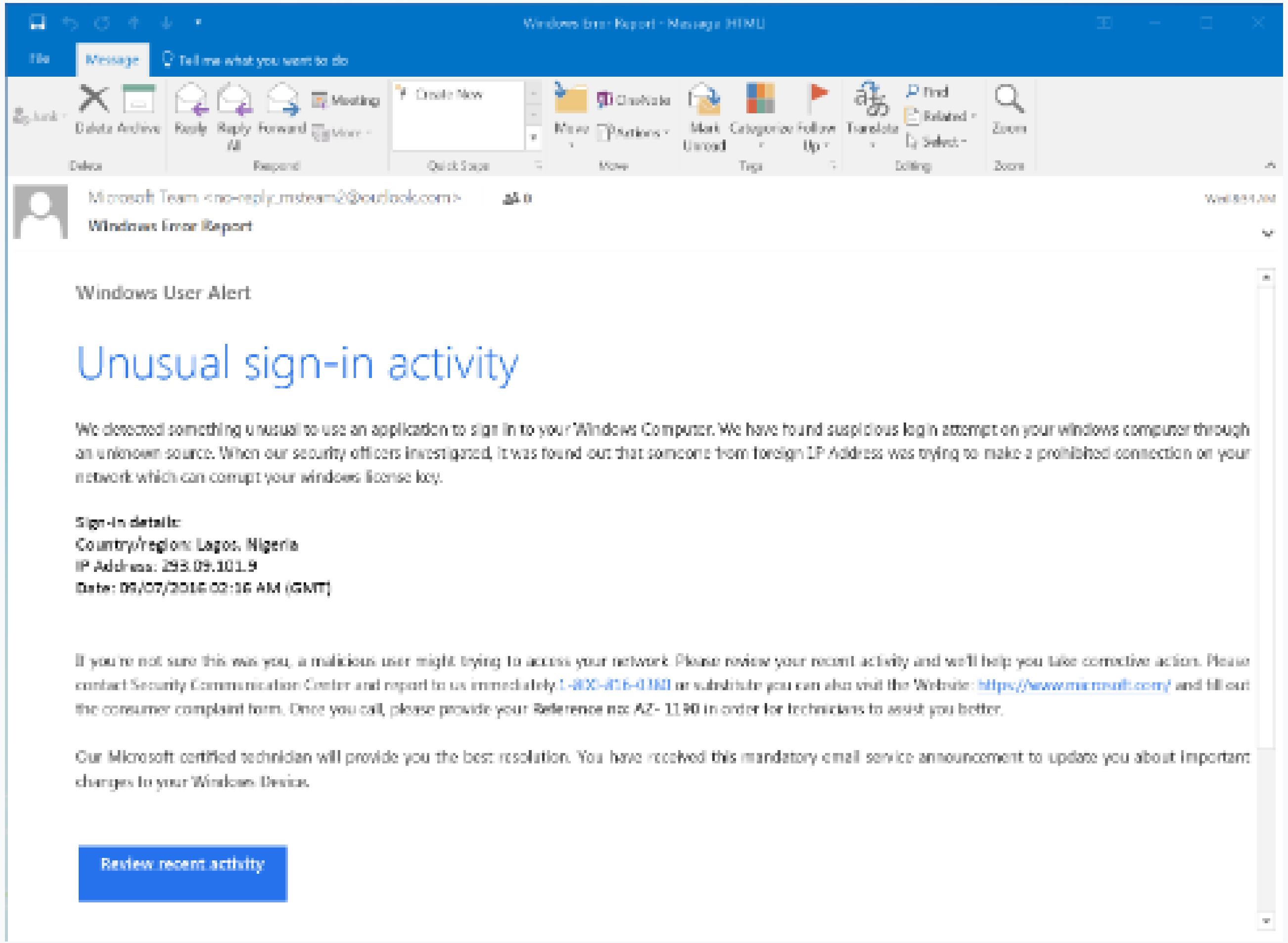
Telecommunications
4.5 billion
compromised records in 2023

Education
Ransomware attacks surge, hitting **80% of lower** and **79% of higher** education institutions

Broadband Search

- https://www.broadbandsearch.net/blog/alarming-cybercrime-statistics

The hook: Investigate unusual account activity



Microsoft Team <no-reply_msteam2@outlook.com>

Windows Error Report

Windows User Alert

Unusual sign-in activity

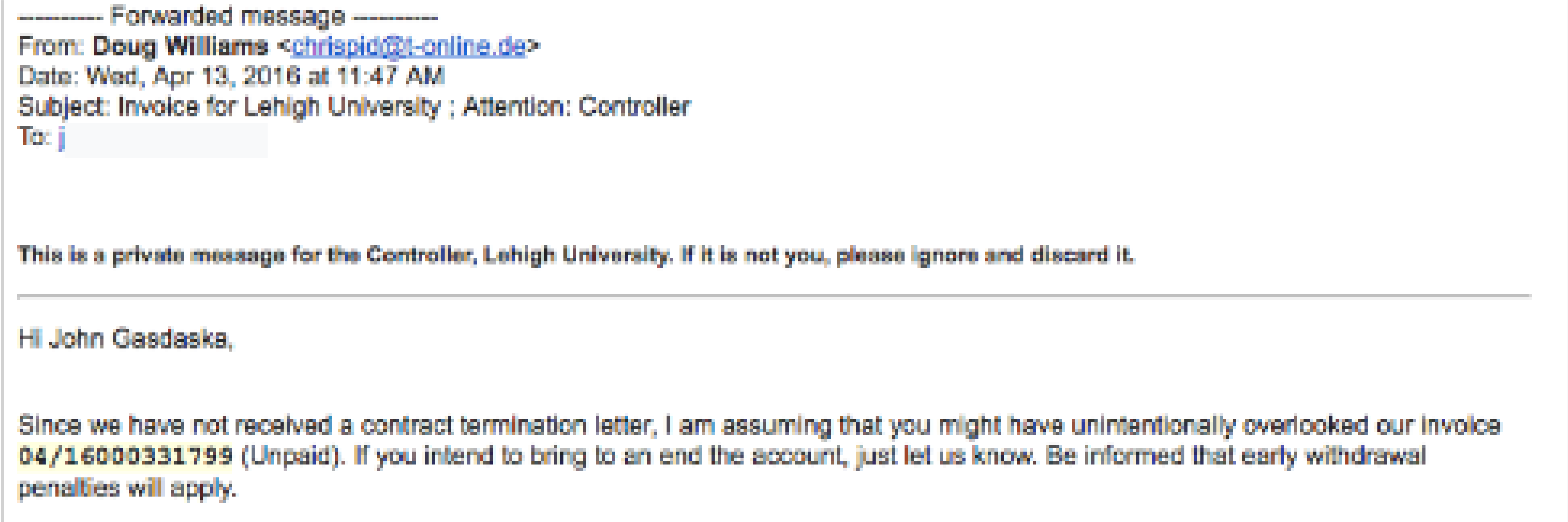
We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign IP Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately 1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your Reference no: AZ- 1190 in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

The hook: Complete invoice payment or face penalties

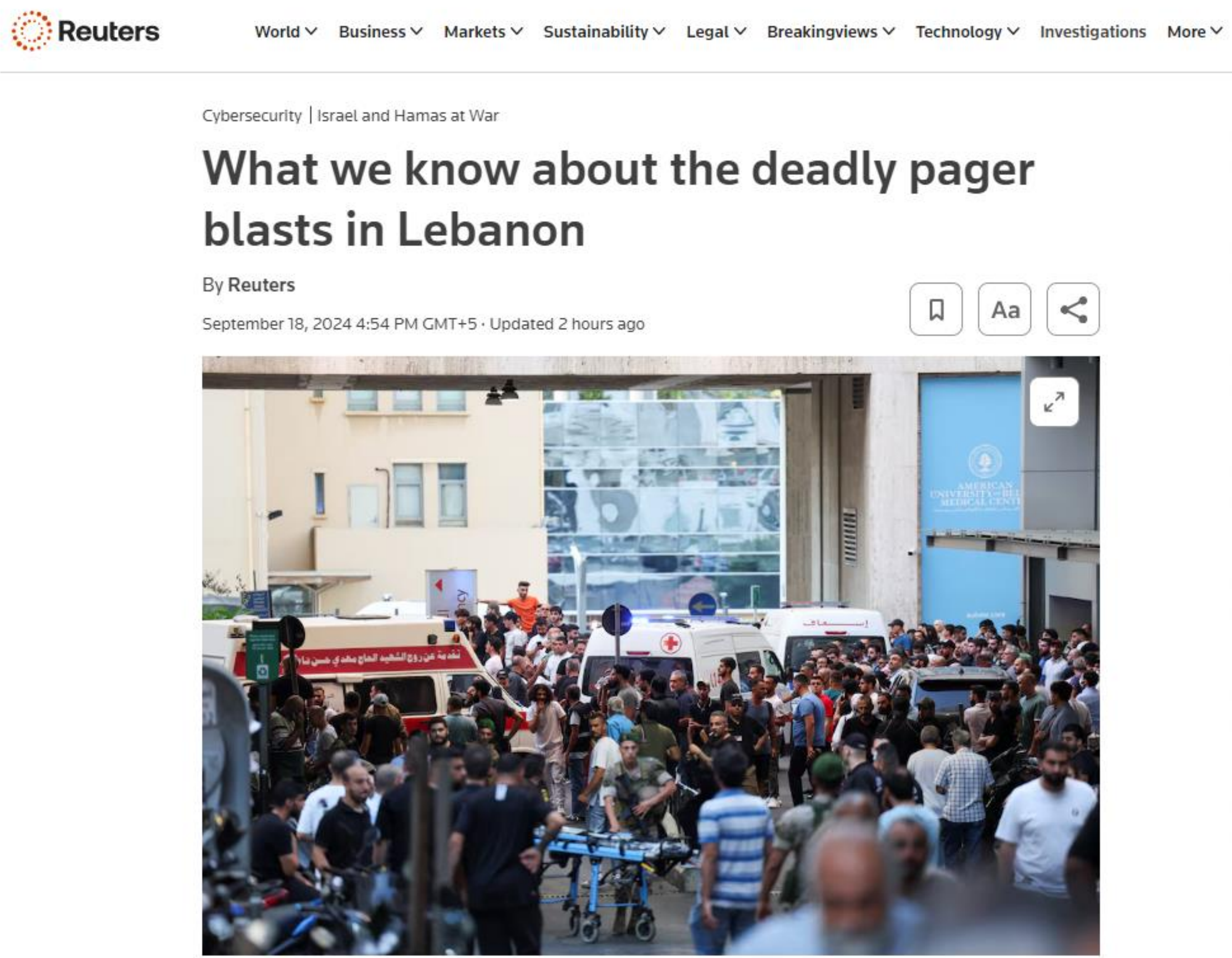


---------- Forwarded message ----------
From: **Doug Williams** <chrispid@t-online.de>
Date: Wed, Apr 13, 2016 at 11:47 AM
Subject: Invoice for Lehigh University ; Attention: Controller
To: j[redacted]

This is a private message for the Controller, Lehigh University. If it is not you, please ignore and discard it.

Hi John Gasdaska,

Since we have not received a contract termination letter, I am assuming that you might have unintentionally overlooked our invoice `04/16000331799` (Unpaid). If you intend to bring to an end the account, just let us know. Be informed that early withdrawal penalties will apply.

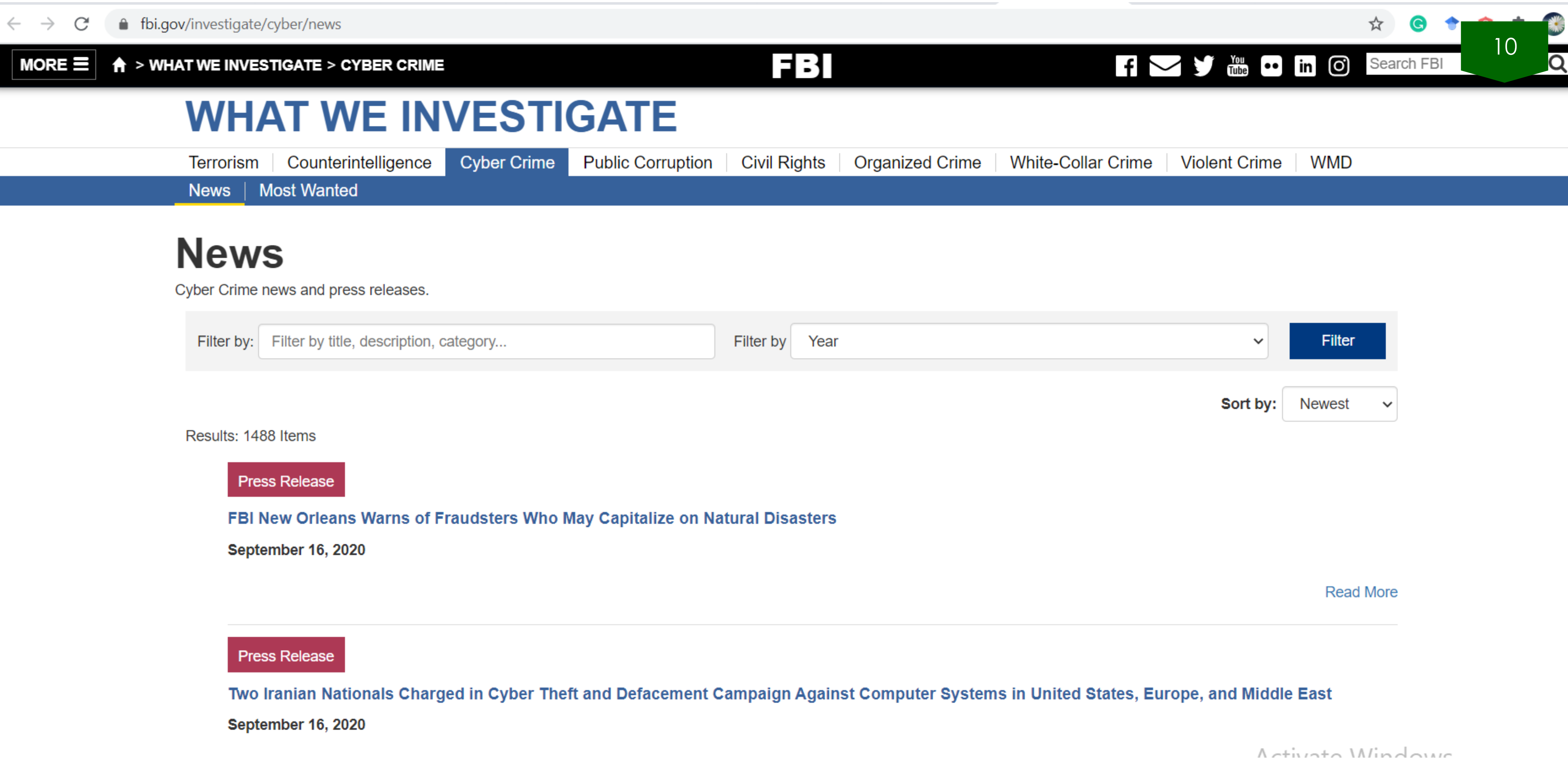


Cybersecurity | Israel and Hamas at War

What we know about the deadly pager blasts in Lebanon

By Reuters

September 18, 2024 4:54 PM GMT+5 · Updated 2 hours ago



News

Cyber Crime news and press releases.

Results: 1488 Items

Press Release

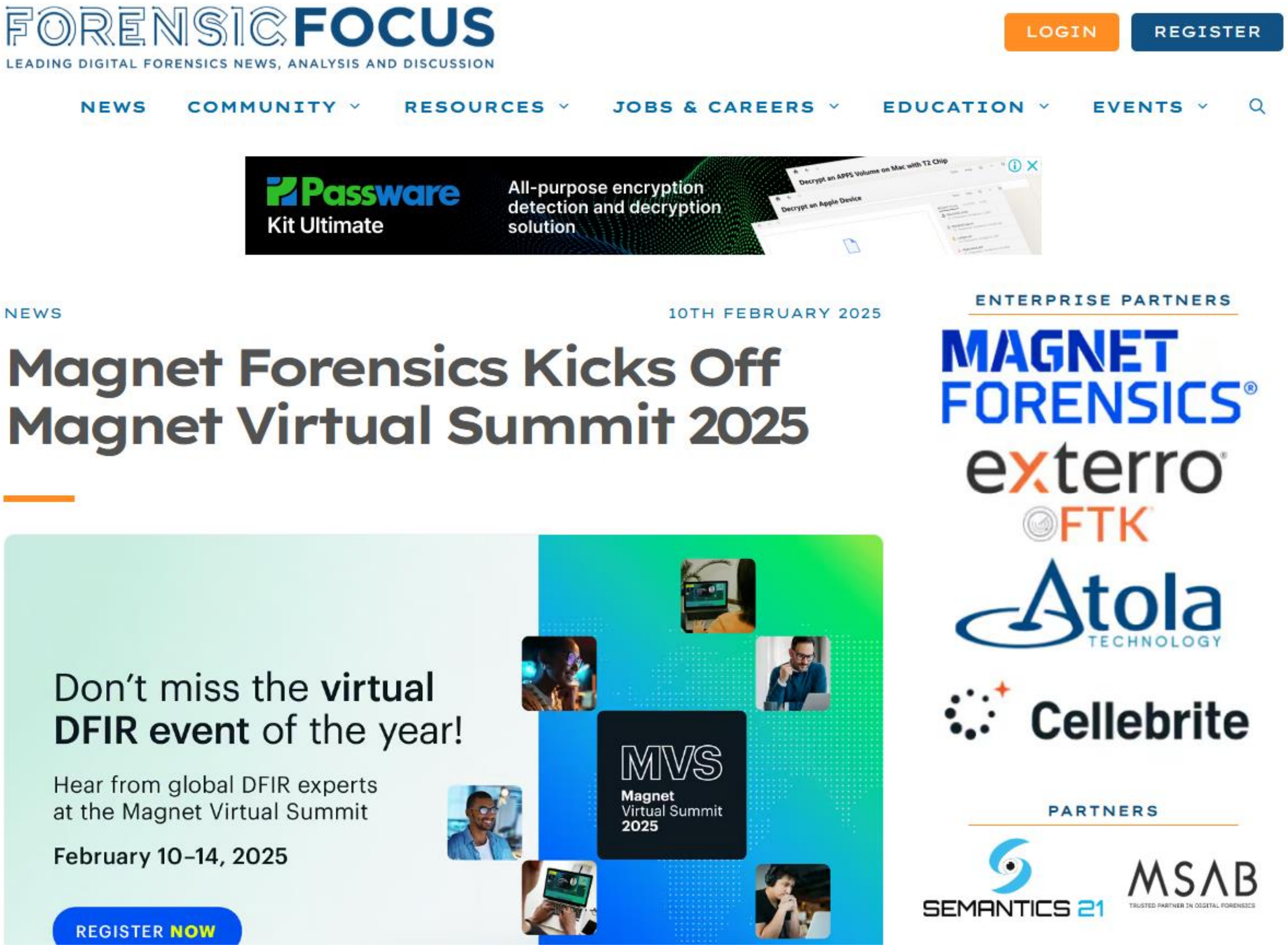
FBI New Orleans Warns of Fraudsters Who May Capitalize on Natural Disasters

September 16, 2020

Press Release

Two Iranian Nationals Charged in Cyber Theft and Defacement Campaign Against Computer Systems in United States, Europe, and Middle East

September 16, 2020



NEWS

10TH FEBRUARY 2025

Magnet Forensics Kicks Off Magnet Virtual Summit 2025

Don't miss the **virtual DFIR event** of the year!

Hear from global DFIR experts at the Magnet Virtual Summit

February 10–14, 2025

REGISTER **NOW**

MVS
Magnet
Virtual Summit
2025

ENTERPRISE PARTNERS

PARTNERS

Activity 1 [10 minutes]

ENUMERATION

Group A: Visit FBI website and find 3 interesting facts.

Group B: Visit forensic focus website and find three interesting clues.

Digital Forensics

Definition:

Preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis using well-defined methodologies and procedures.

Methodology:

- Acquire the evidence without altering or damaging the original.
- Authenticate that the recovered evidence is the same as the original seized.
- Analyze the data without modifying it.

The global Digital Forensics market size was valued at **US$ 2453.06 million in 2022** and is expected to expand at a CAGR of 13.38% during the forecast period, reaching **US$ 5211.15 million by 2031**.

Digital Forensics (NIST)

National Institute of Standards and Technology (NIST) defines

digital forensics

as

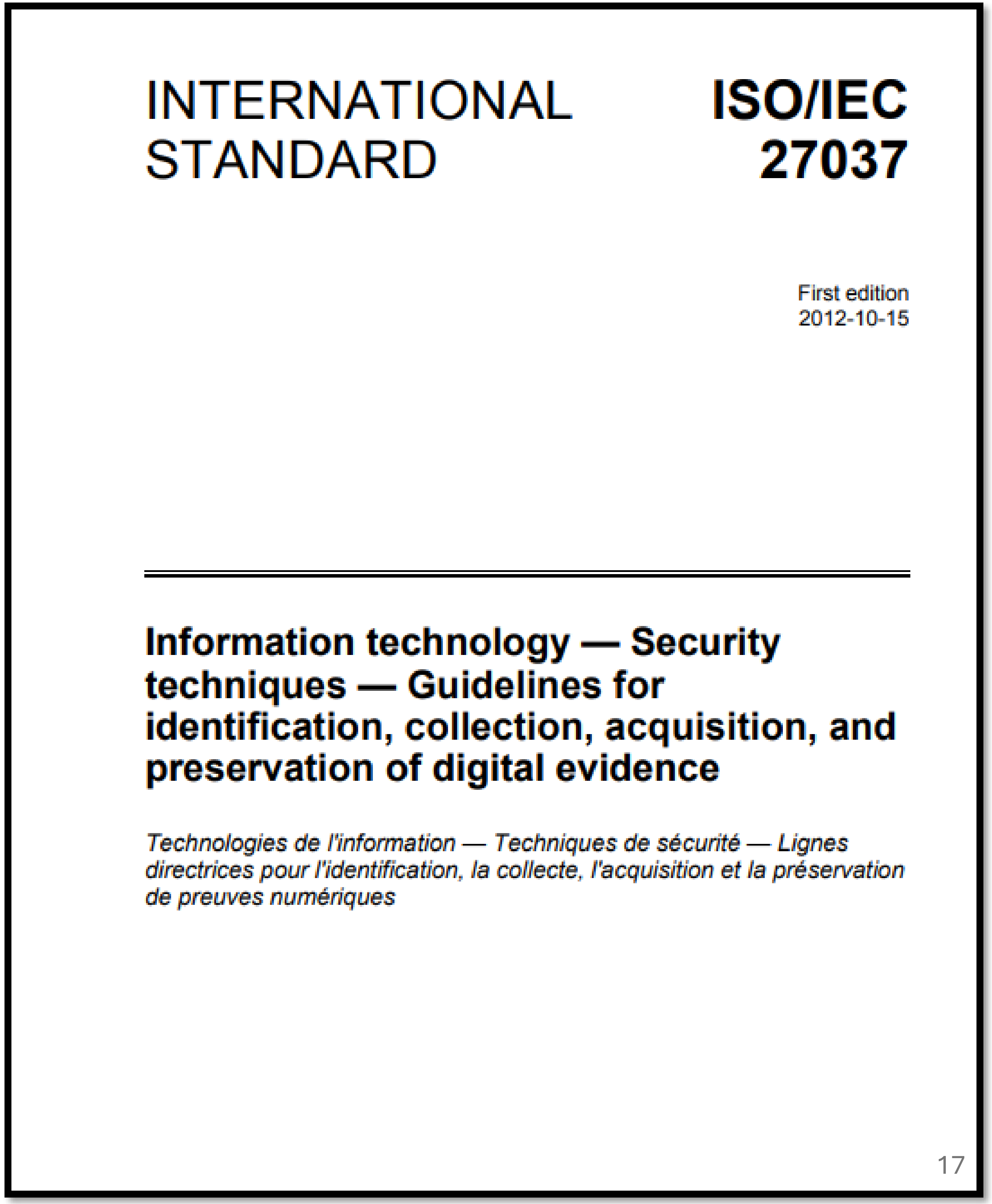
“the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.”

Activity 2 [10 minutes]

1. Form a group of three.
2. Discuss and document details about:
   - Interesting cybercrime (may be personal experience)
   - How the investigation of the cybercrime was conducted (or how it could have been investigated).
3. Prepare to present your findings to the class.

Reading Task

Digital Forensics Framework



INTERNATIONAL STANDARD

ISO/IEC 27037

First edition
2012-10-15

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

Links to explore

- https://www.sans.org/digital-forensics-incident-response/
- https://www.journals.elsevier.com/forensic-science-international-digital-investigation
- https://link.springer.com/chapter/10.1007/978-981-15-1480-7_20
- https://www.nist.gov/news-events/news/2020/06/nist-digital-forensics-experts-show-us-what-you-got
- https://www.computer.org/publications/tech-news/research/digital-forensics-security-challenges-cybercrime