

The background features a dark, textured surface with a pattern of glowing orange binary digits (0s and 1s) arranged in a grid-like fashion. A large, stylized orange arrow points diagonally upwards from the bottom left towards the top right, passing behind the text.

# **Cyber-Threats: Are Libraries Safe?**

# Poll the Audience

- Have you been affected by a data breach?
- How many have had their identity stolen?
- Has personal information been stolen?

# What is Cybersecurity?

- **Cybersecurity** refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.

# Agenda

- Personally Identifiable Information (PII)
- Open-Source Intelligence (OSINT)
- Social Engineering
  - Phishing
- Ransomware
- Countermeasures

# OMB M-07-168

- The Office of Management and Budget (OMB) has issued several memoranda with requirements for how Federal agencies must handle and protect PII
- OMB M-07-168 specifically requires agencies to:
  - Review current holdings of PII and ensure they are accurate, relevant, timely, and complete
  - Reduce PII holdings to the minimum necessary for proper performance of agency functions
  - Develop a schedule for periodic review of PII holdings
  - Establish a plan to eliminate the unnecessary collection and use of SSNs

# NIST SP 800-122

- PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) **any other information that is linked or linkable to an individual**, such as medical, educational, financial, and employment information.
- Information about an individual that is **linked or linkable** to one of the above (e.g., date of birth, place of birth, race, religion, **weight**, activities, geographical indicators, employment information, medical information, education information, financial information).

# Linkable Information

- Linked information is information about or related to an individual that is logically associated with other information about the individual. In contrast, linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals ... **if the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable.**

# Social Engineering

- Hacking a target through people
- A target can be:
  - A person
  - A company
  - A website
  - ...etc.
- Large companies spend a lot of time and money securing their systems
- However, these systems are managed and used by **HUMANS**
- Unfortunately, not much is spent on educating employees



# Social Engineering

- Impact on an Organization
  - Economic losses
  - Damage of goodwill
  - Loss of privacy
  - Dangers of terrorism
  - Lawsuits
  - Temporary or permanent closure

# Social Engineering (cont'd)

- Behaviors Vulnerable to Attacks
  - Human nature of trust
  - Ignorance about social engineering
  - Greed
  - Compliance from a sense of moral obligation
  - Fear of loss

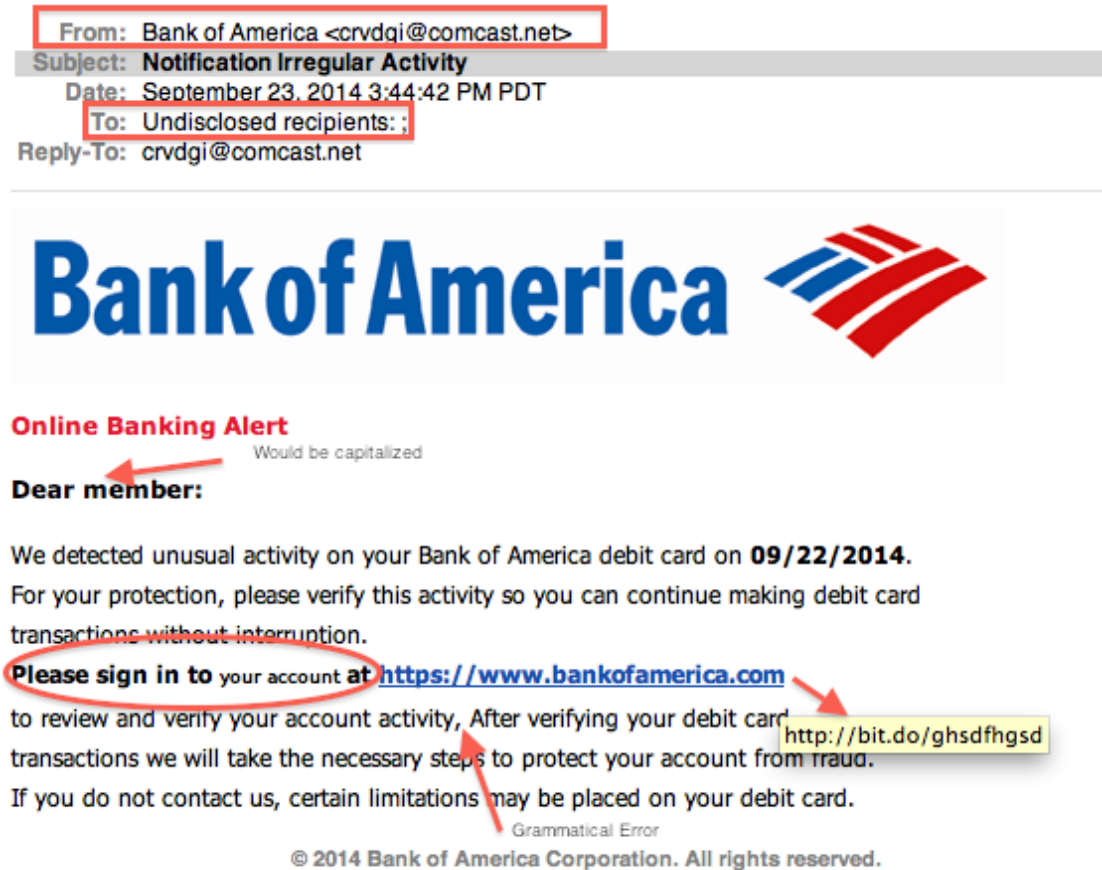
# Social Engineering (cont'd)

- Why is Social Engineering so Effective?
  - **Humans** are the weakest link
  - Social engineering attempts are difficult to detect
  - There is no specific software or hardware that can defend against social engineering attacks
  - There are no specific methods that can be applied to ensure complete protection against social engineering attacks

# Email Phishing

- Investigate the Display Name
- Check the Header From Email Address
- Review The Salutation
- Urgent or Threatening Language
- Don't Give up Personal or Company Confidential Information
- Look But Don't Click
- No Clicking on Attachments Either!
- Spelling Mistakes
- The Signature Line
- Be a Skeptic

Easy, right?!



# Email Phishing (cont'd)

- What about this one?!



We noticed unusual activity in your [PayPal](#) account.

Dear [REDACTED]

We need your help resolving an issue with your [PayPal](#) account. Until you help us resolve this issue, we've temporarily limited what you can do with your account.

Please log in to your [PayPal](#) account and complete the steps to confirm your identity and recent account activity. To help protect your account, access will remain limited until you complete the necessary steps.

[Review your account](#)

Forgot your email or password? [Recover them here](#)

## RETURN SHIPPING'S ON US.

Sending something back? PayPal can cover your return shipping costs. [See limitations](#)

[Learn More](#)

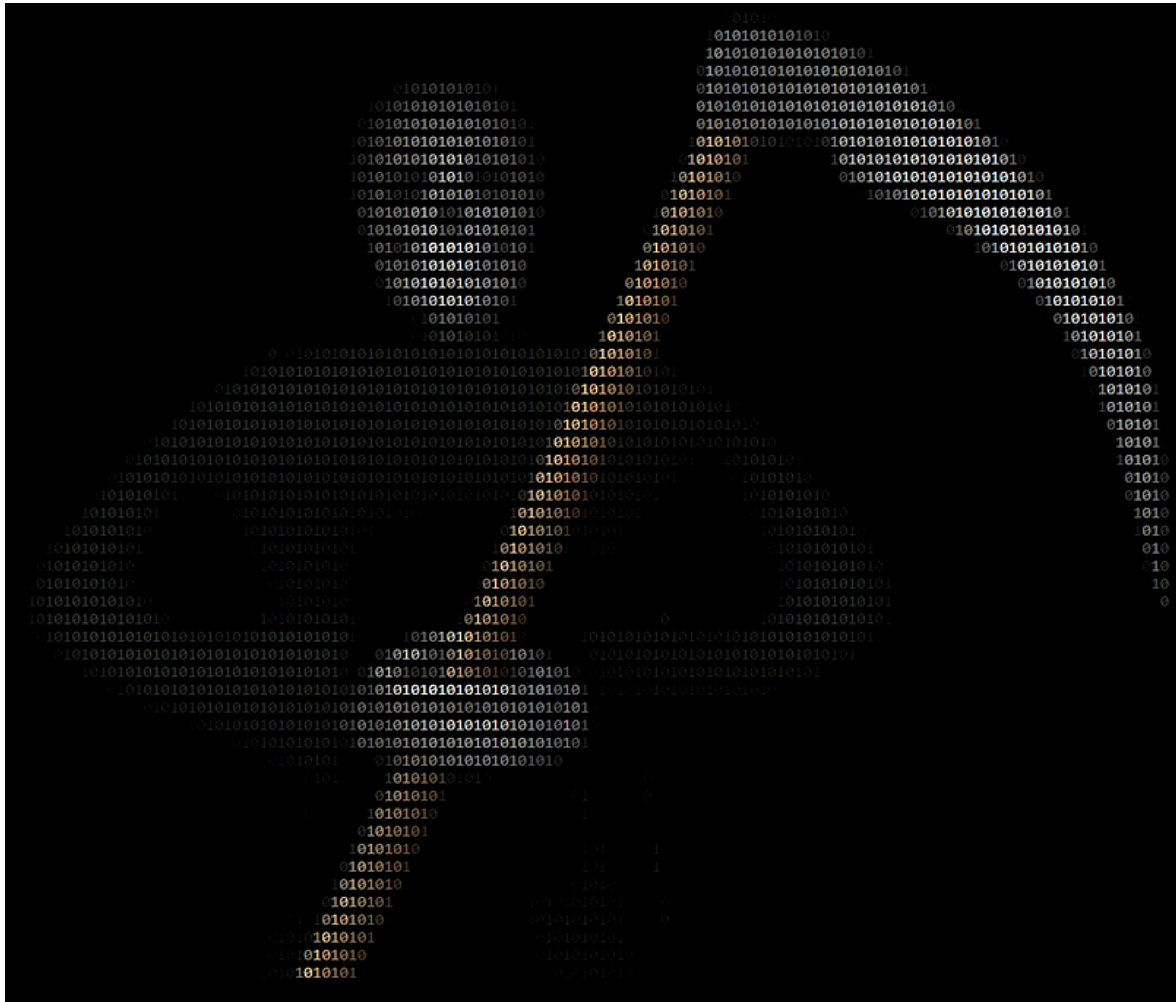
[Account](#) [Help](#) [Fees](#) [Privacy/Cookies](#) [Apps](#) [Shop](#)



Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any [PayPal](#) page or email.

Copyright © 2017 [PayPal](#), Inc. All rights reserved. [PayPal](#) is located at [2211 N. First St., San Jose, CA 95131](#).

# Ransomware



## What is Ransomware?

Ransomware is essentially digital extortion that uses encryption to keep files and systems locked and holds them “hostage” until a payment has been made.

- WannaCry
- Petya
- Bad Rabbit
- LockerGoga
- SamSam

# Oh, Really ...

“In particular, the library confirmed that the ONLY personal data it retained were patron names, phone numbers, and addresses—no credit card or Social Security information.”

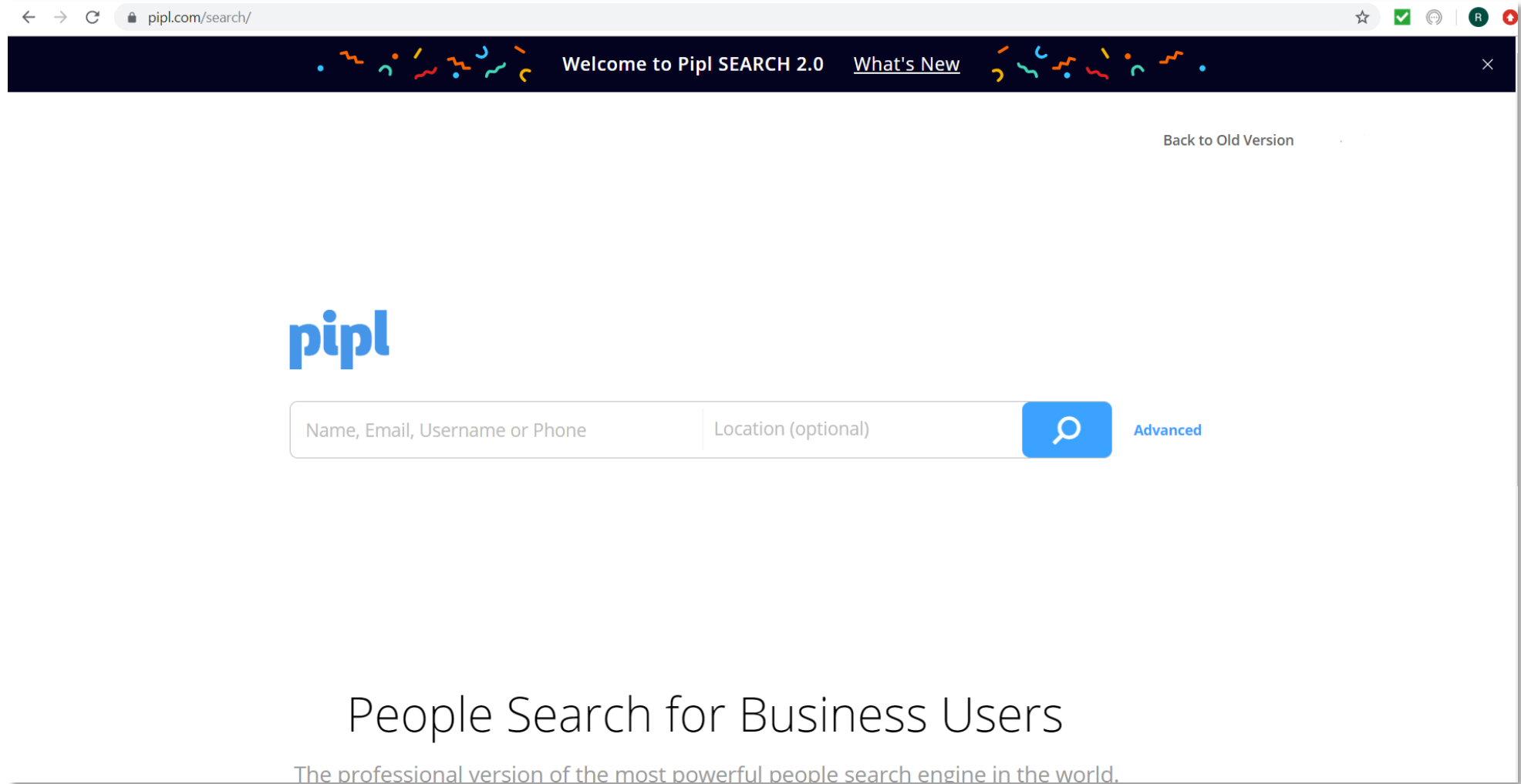
- American Libraries Magazine, 6/1/2018

# OSINT

- Open-Source Intelligence (OSINT)
  - Advanced Searches
    - Shodan.io
    - Hunter.io
  - PIPL
  - WeLeakInfo
  - The Harvester
  - Maltego



# PIPL



The screenshot shows the PIPL SEARCH 2.0 website. At the top, a dark blue header bar contains the text "Welcome to Pipl SEARCH 2.0" and a link to "What's New". Below the header, the PIPL logo is displayed in blue. A search bar is centered on the page, featuring two input fields: "Name, Email, Username or Phone" and "Location (optional)". To the right of the search bar is a blue button with a magnifying glass icon and the text "Advanced". Below the search bar, the text "People Search for Business Users" is displayed, followed by the tagline "The professional version of the most powerful people search engine in the world."

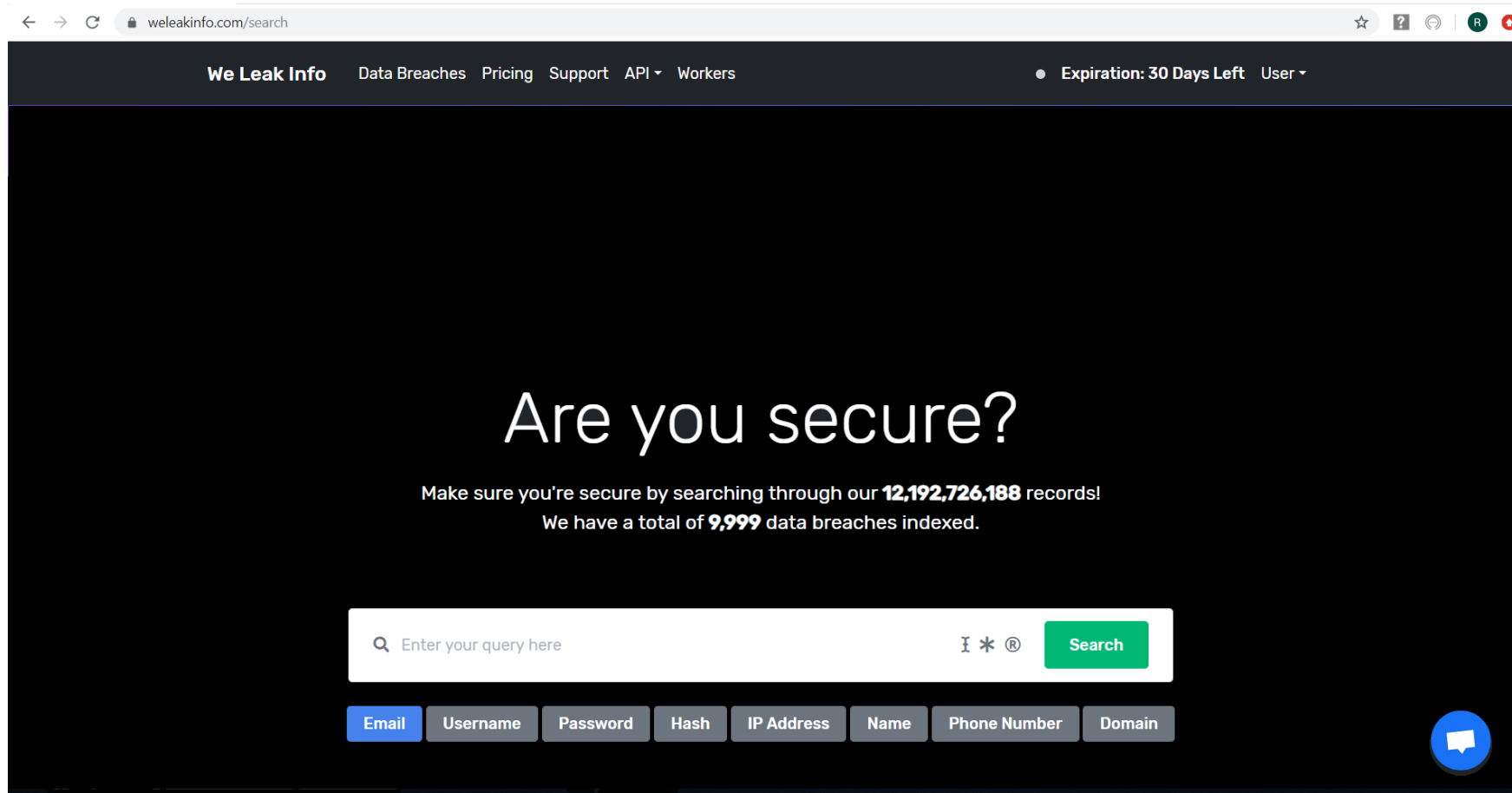
pipl

Name, Email, Username or Phone Location (optional) Advanced

People Search for Business Users

The professional version of the most powerful people search engine in the world.

# We Leak Info

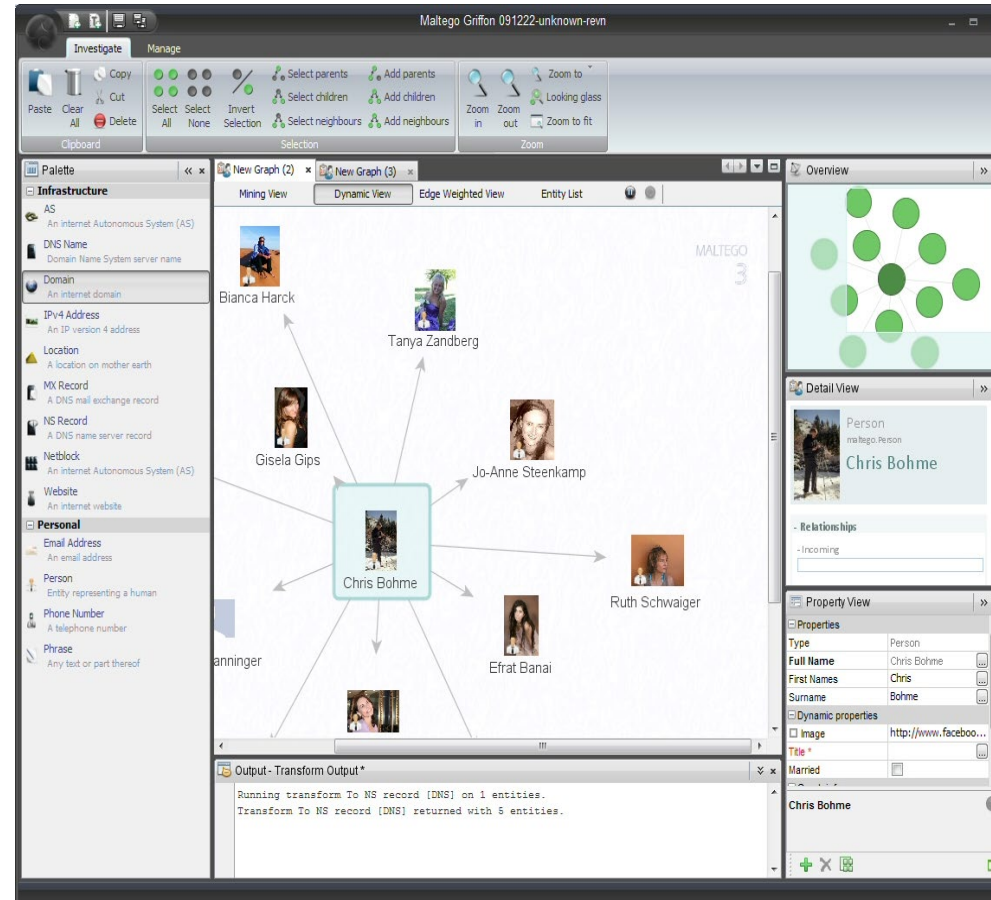


# The Harvester

[illegible]

# Maltego

- Maltego can be used to determine the relationships between the following entities:
- People.
  - Names.
  - Email addresses.
  - Aliases.
- Groups of people (social networks).
- Companies.
- Organizations.
- Web sites.
- Internet infrastructure such as:
  - Domains.
  - DNS names.
  - Netblocks.
  - IP addresses.
- Affiliations.
- Documents and files.



# Demo

# Countermeasures

- Annual Training
- Security Policies
- Maintaining Privacy

# Security Policies

- User Account Policy
- Password Policy
- Information Protection Policy
- Email Security Policy
- Acceptable Use Policy
- Password Policy
- Privacy Policy
- Social Media Policy

# Privacy

- Use strong, unique passwords
- Set up two factor authentication on everything
- Public Wi-Fi networks are a big 'no'
  - Use your phone's data for better security
- Use a TOR browser
- Be mindful of every app you install



*Ruth Capezzone*

**ruth@irradienttech.com**