CRIMINAL INVESTIGATION

Matthew Bohlmann
National ID Theft Program Manager
IRS-CI – Refund Crimes

January 11, 2021

IRS-CI Mission

Investigate criminal violations of the Internal Revenue Code and related financial crimes

Foster confidence in the tax system and compliance with the law

Business Email Compromise (BEC)

Data Breach

What is the Problem?

BEC – Business Email Compromise

2019: 23,775 complaints

$1.7 Billion in adjusted losses

IRS – Reported Data Breach Incidents

146 Incidents Reported; over 118,000 TINs

Over $15 Million in Revenue

BEC

- **Cybercriminals are able to identify chief operating officers, school executives or others in position of authority (Social Engineering).**
- **Fraudsters mask themselves as executives or people in authoritative positions and send emails to payroll or human resources requesting copies of Forms W-2. (Grooming)**
- **Form W-2 contains the following (Exchange of Information)**

  Employment Identification Numbers (EIN)

  Social Security Numbers

  Income / Withholdings (Federal, State, Local)

  Address, Retirement Plan, Health Benefits Plan, etc.

EXAMPLE

DL

Diane Larson <d.larson@healthyemployee.me> [redacted] 11:21 AM

Free flu shots for you and your family

Retention Policy Delete Deleted Items after 365 days (1 year) Expires 01/27/2040

This message was sent with High importance.

Free Flu Shots!

Dear Employees and Contractors,

This year's flu season is almost upon us, and we want you to stay healty! The agency has partnered with us to provide free on-site clinics to all employees and their immediate family members.

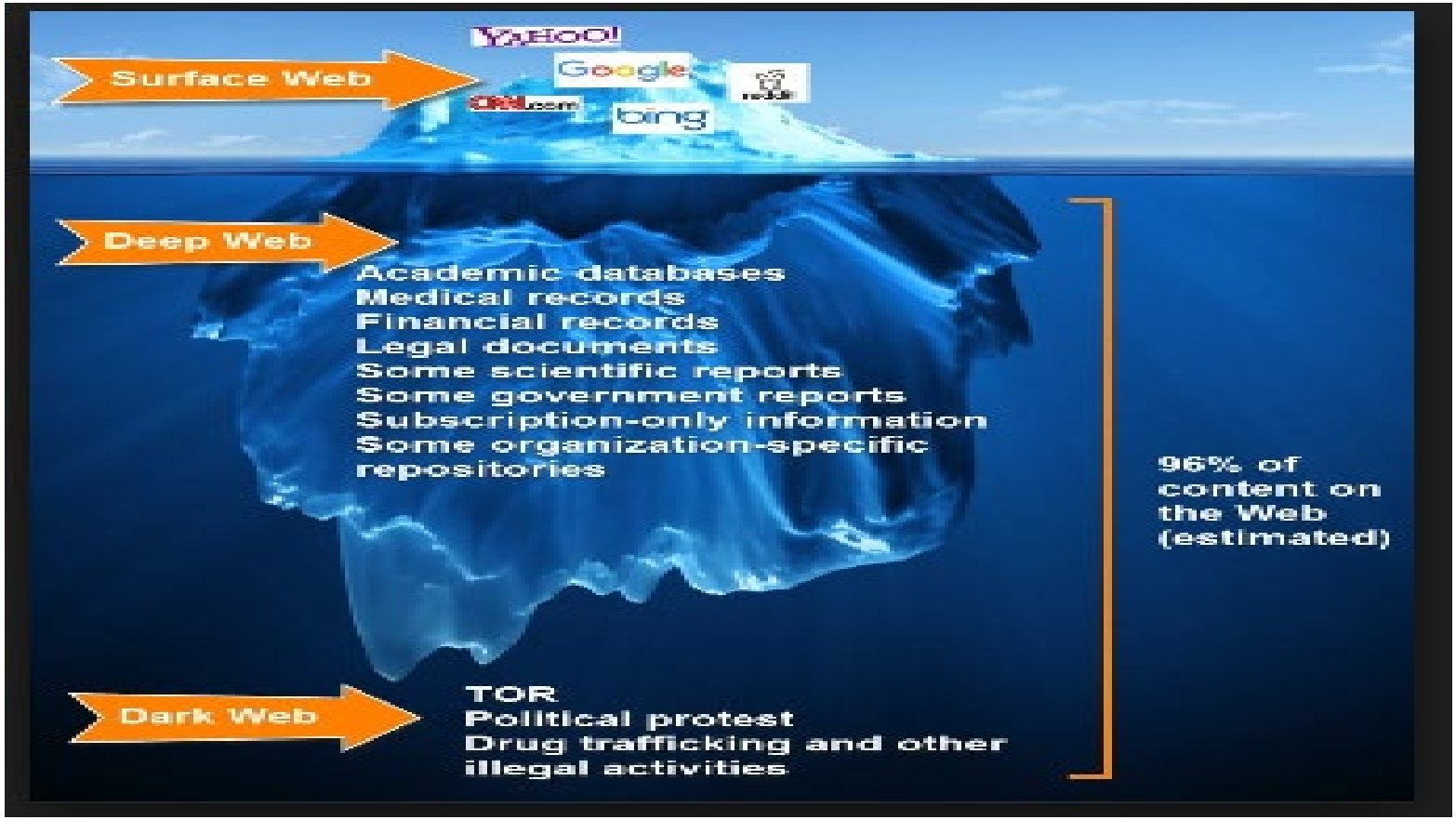
You can view schedules for each site here.

Diane Larson
Sr. Clinician Manager
DNP, RN, FNP-C
HEALTHIEREmployees

Ransomware

- Usually comes in the form of Phishing email and has attachments or links.
- Ransomware is a type of malware that restricts access to infected computers and requires victims to pay a ransom to regain access to their data
- Typical ransoms are in the range of $100 - $300, and are often demanded in the form of digital currency, such as Bitcoin

DARK WEB


Surface Web
Deep Web
Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription-only information
Some organization-specific repositories
Dark Web
TOR
Political protest
Drug trafficking and other illegal activities
96% of content on the Web (estimated)

VIRTUAL CURRENCY

MOST POPULAR – BITCOIN

Currently - over 5,000 Cryptocurrencies in circulation with a market value of approx. $260B

26% of Crypto-Asset founders are located in US

Beware of scammers

Beware of scams and identity theft schemes by criminals around holiday shopping, the approaching tax season, and coronavirus concerns.

Top Tips:

- ✓ Use security software (e.g. antivirus) and keep it updated.
- ✓ Don't open links or attachments on suspicious emails. Fraud scams related to COVID-19 and the Economic Impact Payment are common.
- ✓ Use strong and unique passwords for online accounts.
- ✓ Use multi-factor authentication whenever possible.
- ✓ Shop at sites where the web address begins with "https" and look for the padlock icon.
- ✓ Don't shop on unsecured public Wi-Fi in places like a mall.
- ✓ Secure home Wi-Fis networks with a password.
- ✓ Back up files on computers and mobile phones.

WHAT CAN YOU DO?

- ✓ Do not use the “Reply” option to respond to any business e-mails asking for PII
- ✓ Educate your employees, and then educate again
- ✓ Be careful what you post to social media and company websites
- ✓ Be suspicious of requests for secrecy or pressure to “take action quickly”
- ✓ Carefully scrutinize all e-mail requests for PII or financial transactions

I MESSED UP, NOW WHAT?

- ✓ **Do NOT Panic – Act Quickly**
  - ✓ Notify Internally – supervisors, IT Department, etc.
  - ✓ Notify IRS – Stakeholder Liaison Office

    www.irs.gov – search “stakeholder liaison”

The longer you wait, advantage to the hacker!

More to do…

actual loss of W-2 information
e-mail IRS - dataloss@irs.gov

no actual loss of W-2 information
e-mail IRS - phishing@irs.gov

Lost Payroll data can impact State Agencies
e-mail the Federation of Tax Administrators –
StateAlert@taxadmin.org

More to do…

File a complaint with the Internet Crime Complaint Center (IC3) operated by the Federal Bureau of Investigation.

www.ic3.gov

Contact Local Police or Other Law Enforcement

Report Compromise to Federal Trade Commission

www.identitytheft.gov

Personal ID Theft

Electronic Return Rejected

Verification Letters (5071C, 4883C, and others)

Response to Filed Return

Receipt of US Treasury Refund Check

Receipt of Reloadable Prepaid Card

Receipt of Refund Transfer Company Check

Your Return Preparer informs you of breach

Who do I contact?

On-Line Resource

www.irs.gov – search “identity theft”

File Form 14039 – ID Theft Affidavit

Local Authorities

Credit Agencies

IP PIN

Starting in January, the IRS will offer an Identity Protection PIN to all taxpayers who have been victims of identity theft and can properly verify their identities.

What is it?

The IP PIN is a six-digit number to help prevent the misuse of their Social Security number on fraudulent federal income tax returns. When you have this special code, it prevents someone else from filing a tax return with your Social Security number.

What is the process to register?

The online Get An IP PIN tool at irs.gov/ippin immediately displays the taxpayer's IP PIN. IRS Secure Access will verify your identity with the following:

- Email address
- Social Security Number (SSN) or Individual Tax Identification Number (ITIN)
- Tax filing status and mailing address
- One financial account number linked to your name such as a credit card, student loan, mortgage, auto loan, etc.
- Mobile phone linked to your name or ability to receive an activation code by mail

Multifactor authentication (MFA)

The IRS announced that MFA will be available on all 2021 online tax preparation products.

What is MFA?

A user needs two or more “factors”, such as their credentials (username and password) plus a one-time passcode texted to their mobile phone, in order to log in to a service. It’s also called two-factor authentication or two-step authentication.

Who is using it?

Some online tax preparation products previously offered multi-factor authentication. However, for 2021 all providers agreed to make it a standard feature and all agreed that it would meet requirements set by the National Institute of Standards and Technology.

Why is it important?

MFA is a huge deterrent for criminals since they usually don’t have access to more than one of a user’s login factors. It’s an easy and critical part of securing your and your clients’ data.

Business identity theft

Businesses, just like individuals, can be victims of identity theft. More than 70% of cyberattacks are aimed at businesses with 100 or fewer employees. Thieves may target credit card information, business identity information, or employee identity information.

Resources for business identity theft:

- ✓ IRS related scams may be sent to phishing@irs.gov.
- ✓ Check out the FTC's Cybersecurity for Small Businesses.
- ✓ IRS' new Form 14039-B, Business Identity Theft Affidavit PDF will allow companies to proactively report possible identity theft to the IRS when, for example, the e-filed tax return is rejected.
- ✓ There is a special reporting procedure for employers who experience the W-2 scam. It also may be found at Identity Theft Central's Business section.
- ✓ Remind your payroll clients to keep their EIN application information current. Changes of address or responsible party may be reported using Form 8822-B. Reminder: changes in the responsible party must be reported to the IRS within 60 days.

Telework scams

The IRS closed Tax Security Awareness week with a warning to all tax professionals that they face additional challenges from cybercriminals seeking to exploit COVID-19 fears. Watch for an increase in phishing and hacking, and remember, it CAN happen to you!

The need for a security plan and data theft plan

Even if the FTC Safeguards Rule does not legally apply, it's best practice to have a **data security plan** in place. Be sure to:

- ✓ Include the names of all information security program managers.
- ✓ Identify all risks to customer information.
- ✓ Evaluate risks and current safety measures.
- ✓ Design a program to protect data. See https://www.irs.gov/pub/irs-pdf/p4557.pdf
- ✓ Regularly monitor and test the program.

Also consider an **incident response plan** to have in place in case you experience a breach and data theft.

CURRENT TRENDS

- ✓ Unemployment Compensation
- ✓ Economic Impact Payments
- ✓ PPP Loans
- ✓ Synthetic Identity Theft
- ✓ Initial Coin Offerings
- ✓ Business Identity Theft
- ✓ Telework Scams

ALABAMA CONTACT

David R. McDaniel, Special Agent

Atlanta Field Office – Montgomery, AL

Office: (334) 309-2837

Gary V. Traina, Special Agent

Atlanta Field Office – Mobile, AL

Office: (251) 341-5980

Thank You!

Matthew Bohlmann – 217-993-6603