Let’s Take a Phishing Trip

2024 FAMIS Conference

SKYWARD®

Agenda

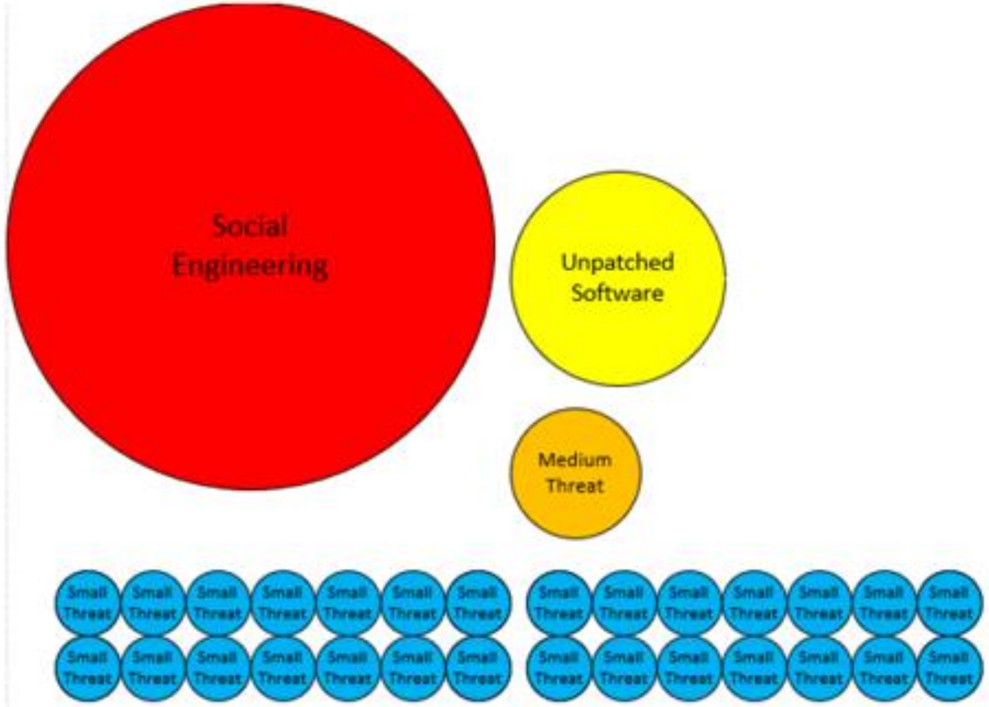
- Why is Phishing Popular?
- Let’s go Phish!
- Phish Identification Made Easy

How Hackers and Malware Break In

- Programming Bug (patch available or not available)
- Social Engineering
- Authentication Attack
- Human / Error / Misconfiguration
- Eavesdropping / MitM
- Side Channel / Information Leak
- Brute Force / Computational
- Injection
- Data / Network Traffic Malformation
- Insider Attack
- 3rd Party Reliance Issue (supply chain / vendor / partner / etc)
- Physical Attack

Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software
- But don’t trust me, measure your own risk



Social engineering is responsible for majority of malicious data breaches.

https://blog.knowbe4.com/phishing-remains-the-most-common-form-of-attack
https://info.knowbe4.com/threat-intelligence-to-build-your-data-driven-defense

Best Defenses

Top Defenses for All People and Organizations

- **Mitigate Social Engineering**
- **Patch Internet-accessible software**
- **Use Multifactor Authentication (MFA) / Non-Guessable Passwords**
  - Use non-phishable FA where you can. Where you can't...
  - Use unique, unguessable, different passwords for every website and service
- **Teach Yourself and Everyone How to Spot Rogue URLs**
  - https://blog.knowbe4.com/top-12-most-common-rogues-url-tricks
  - https://info.knowbe4.com/rogue-urls

Social Engineering Tactics

- **Phishing - Email**
- **Smishing - SMS**
- **Spoofing - Fake websites**
- **Brushing - Fake orders, invoices**
- **Disinformation Campaigns**
  - Spread and utilizes false information / creates fear

Phishing Tactics

Phishing

- Spray & Pray

Spear-Phishing

- Target to individuals or small groups with common interests
- Most common attack

Whaling

- Targeting the “big” phish
- School Board / Leadership

Let's go Phish!

Phishing Trip: Etiquette

Phishing Etiquette

Are Schools, Hospitals, & Critical Infrastructure fair game?

Is there honor among thieves?

Yes & No

Bad Actors / APTs make their own rules

Phishing Trip: Etiquette

Phishing Etiquette

What if you catch a phish that's "too big"?

Cut the line…give away the encryption key?

OR

Reel in the big one!

Phishing Trip: Tacklebox Preparation

Hire a charter?

Phishing as a Service (PaaS)?

- Initial Access Broker
- Phishing Kits
- No developer skills required
- Shared Revenue model

No Phishing license required!!

Phishing Trip: Tacklebox Preparation

No Phishing license required!!

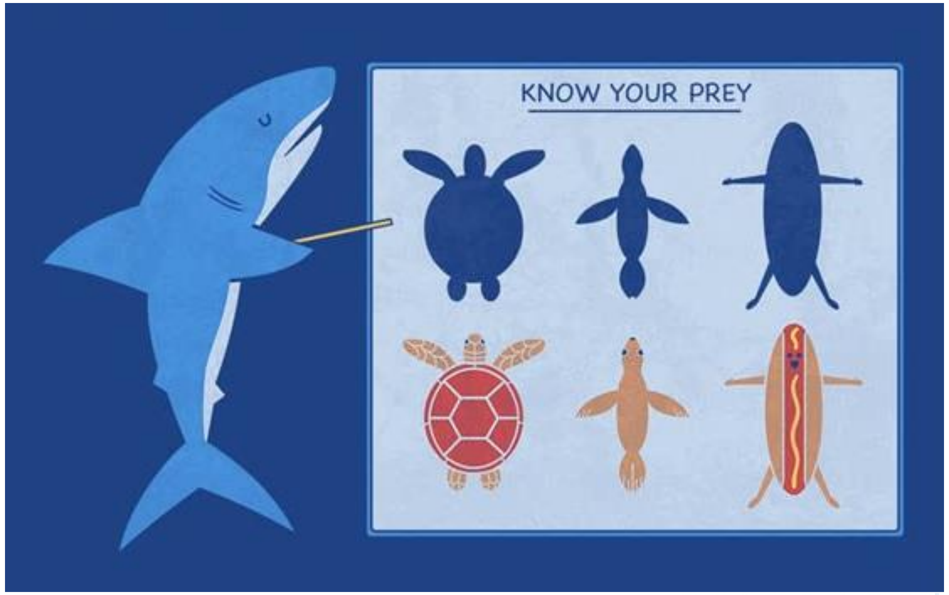
Do it yourself?

Advanced Persistent Threat (APT)

- Develops own Phishing tools
- Fake Domains, Websites, email relay/accounts, Infrastructure
- Managers / Employees / Human Resources

Phishing Trip: Choose Your Prey

- Social Media – any public information is fair game
- Dark Web – Private information can be fair game
- Current Events (events, news, disasters, etc.)
- Misinformation (fake news)



Phishing Trip: Choose your Lures & Bait

What triggers work best for your prey?

Manipulate Emotions

- Urgency
- Fear
- Curiosity
- Greed
- Sympathy

Impersonation

- Brand / Domain / Vendor
- Someone you trust
- Authority / Executives

Phishing Trip: Choose your Phishing Hole

Where will you Phish?

Evaluate targets

- Likelihood to pay?
- History of ransom payments?
- Security vulnerabilities
- Geopolitical value
- Social Justice value

Phishing Trip: Choose your Gear

Traditional Phishing Gear: Net

- Spray & Pray
- Modern email filters will block most of these attempts
- A small percentage can still be a good catch

Phishing Trip: Choose your Gear

Spear-phishing Gear: Spear

- More effective against modern Email filters
- Over 90% of phishing is Spear-phishing.

Phishing Trip: Choose your Gear

Whaling Gear: Harpoon

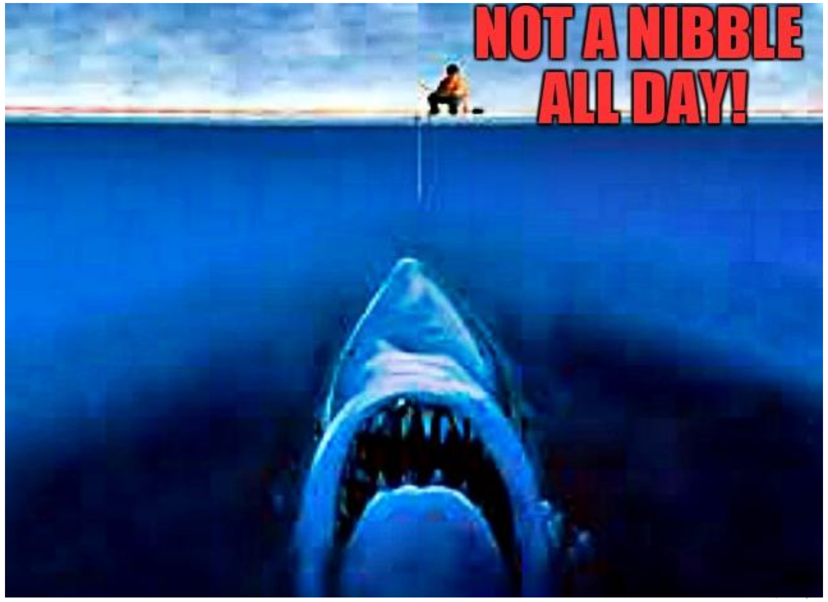
- More effective against modern Email filters
- Catching big phish could be more lucrative

Or use “winter gear” ☺

Phishing Trip: Set the Hook

Watch closely for the first bite…

- Monitor for email replies
- Harvests credentials
- Malware infections that "phone home"
- Joins botnet, sends beacon



Hooked One! What’s Next?

It’s time to land your Phish!

#1 - Business Email Compromise

#2 - Ransomware

Business Email Compromise (BEC)

Business email compromise (BEC) is a type of cybercrime where the scammer uses email to trick someone into sending money or divulging confidential company info. The culprit poses as a trusted figure, then asks for a fake bill to be paid or for sensitive data they can use in another scam.

There were nearly 20,000 BEC complaints to the FBI in 2021, with estimated losses of roughly $2.4 billion.

Playbook 1: Payroll Fraud

- If possible, gain control of several email accounts within the same organization

- Hide legitimate emails from the user(s)

Shhh, Be vewy vewy quiet…..

Playbook 1: Payroll Fraud

Masquerade as the victim

- Request payroll ACH change(s) to a new bank account
- Retrieve the funds
- Close the account
- The heist is complete before the victim asks about the missing paycheck

Playbook 2: Vendor Email Compromise

Masquerade as a Vendor

- Monitor the mailbox for an opportunity (for months, if necessary)
- Hide legitimate emails from the user
- Set up email forwarding rules

Do not tip them off!

Playbook 2: Vendor Email Compromise

- Utilize the relationship / trust, or build trust
- Convince the victim to re-route large ACH payments
- Retrieve the funds
- Close the account
- The heist is complete before the legitimate vendor asks about the missing payment.

BEC: How to Protect Yourself

Implement Safeguards

- Establish more that one communication channel to verify significant transactions
- Remain vigilant of sudden changes in business practices
- Implement Multi-factor authentication
- Raise awareness for individuals responsible for handling money

Victims of BEC Scams

- File with the FBI's Internet Crime Complaint Center (IC3) at www.IC3.gov
- File a claim with your Cyber Insurance
- Contact Victims

Playbook 3: Ransomware

Using the MITRE ATT&CK Framework to Deconstruct a Ransomware Attack

- Attack Phase 1 – RECON (Preparation)
- Attack Phase 2 – INITIAL ACCESS (Phished!)
- Attack Phase 3 – EXECUTION, PERSISTENCE, ESCALATION, EVASION
- Attack Phase 4 – CREDENTIAL ACCESS, DISCOVERY, LATERAL MOVEMENT
- Attack Phase 5 – EXFILTRATION, IMPACT

Playbook 3: Ransomware

Attack Phase 5 – EXFILTRATION

- Sensitive Data is transferred to Attackers
- This data may be used as:
  - Extortion for payment
  - Public Embarrassment
  - Revenge
  - Political reasons
  - Sold on the black market
  - Personal Gain

MITRE
ATT&CK™

Playbook 3: Ransomware

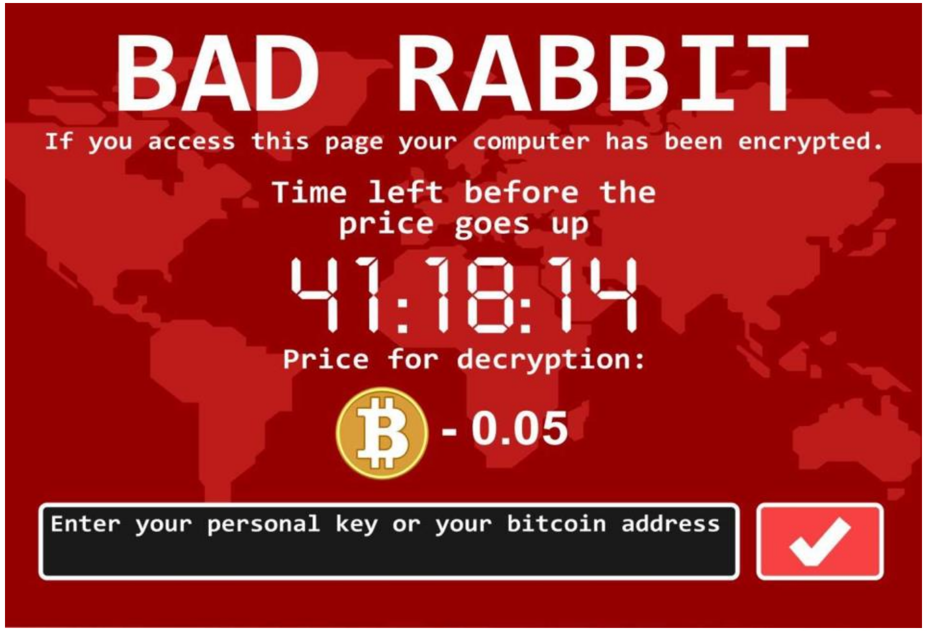
Attack Phase 5 – IMPACT

- Goal: Disrupt!
  - Destroy data
  - Tamper with data
  - Encrypt data
  - Remove account access
  - Deface websites

MITRE
ATT&CK™

Ransomware Notes

- ALWAYS Includes Payment Instructions
- Might include Ransomware variant
- Might include contact information
- You might receive a phone call / text



BAD RABBIT

If you access this page your computer has been encrypted.

Time left before the
price goes up

41:18:14

Price for decryption:

₿ - 0.05

Enter your personal key or your bitcoin address ✓

Ransomware: How to Protect Yourself

Invest in "Most Impactful" Security Measures

- Implement Multi-factor authentication
- Raise awareness for all individuals
- Implement Advanced Endpoint Protection (EDR/XDR)
- Backup often, INCLUDING air-gapped backups
- Consider Cloud Hosting

Victims of Ransomware

- Report ransomware through CISA's Reporting Tool
- File a claim with your Cyber Insurance

Ransomware Resources

CISA K12 Guide → https://www.cisa.gov/k-12-school-security-guide

CISA Stop Ransomware → https://www.cisa.gov/stopransomware

CISA Ransomware Guide → https://www.cisa.gov/stopransomware/ransomware-guide

FBI Ransomware Tips → https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

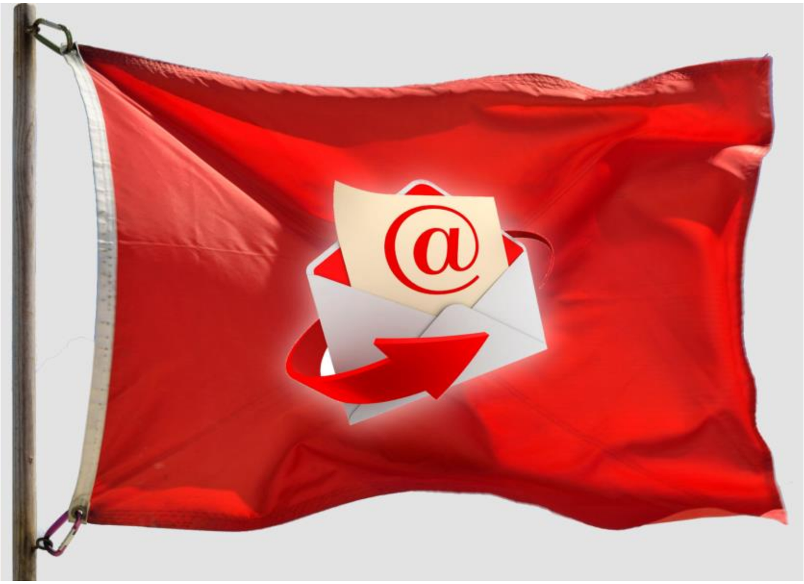
CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

FBI FEDERAL BUREAU
OF INVESTIGATION

Spot the Phish!!!

Learn the Red Flags

- Look at FROM Address
- Hover over HYPERLINKS
- Look at the DATE it was sent
- Stop and think about the SUBJECT and CONTENT
- Look for ATTACHMENTS



Social Engineering Red Flags

FROM

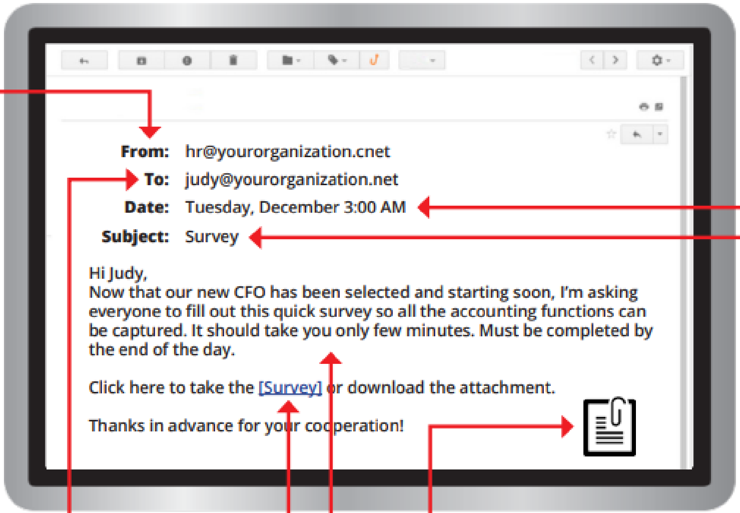
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known website. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



From: hr@yourorganization.cnet
To: judy@yourorganization.net
Date: Tuesday, December 3:00 AM
Subject: Survey

Hi Judy,
Now that our new CFO has been selected and starting soon, I'm asking everyone to fill out this quick survey so all the accounting functions can be captured. It should take you only few minutes. Must be completed by the end of the day.

Click here to take the [Survey] or download the attachment.

Thanks in advance for your cooperation!

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

PROGRESS SOFTWARE

ISCorp Integrated Systems Corporation

Microsoft Authorized Education Partner

KnowBe4 Human error. Conquered.

aruba a Hewlett Packard Enterprise company

Skyward's IT experts have the latest knowledge on industry trends and developments to help keep your network running smoothly.

NETWORK CONSULTING

- Resilient Wired Network Infrastructure
- Complete Wireless Network Solutions
- Virtual Server Design and Support
- Storage Area Network Solutions
- IP Telephony Solutions

SUPPLEMENTAL IT STAFFING

- Onsite and Remote IT Support
- Network Assurance Services

ASSESSMENT SERVICES

- Network / Security
- Disaster Recovery
- Secure Cloud Computing

SKYWARD OPTIMIZATION

- Managed Services
- Database Tune-ups
- Remote Update Services
- System Admin Training

NETWORK SECURITY SOLUTIONS

- Intrusion Detection, Prevention, and Next Generation Firewalls
- Email Filtering, Archiving, and Security Solutions
- Internet Filtering and Monitoring Solutions
- On-Staff Security Experts

DISASTER RECOVERY SERVICES

- Skyward Disaster Recovery from ISCorp
- Onsite Data Center Disaster Recovery Solutions

ARCTIC WOLF

FORTINET

Extreme networks

vmware

Mitel

Verkada

TEA Texas Education Agency

APC by Schneider Electric

SONICWALL

BARRACUDA NETWORKS

GeoTrust powered by digicert

veeam

Lightspeed Systems | Partners

Hewlett Packard Enterprise

TOOLS4EVER IDENTITY GOVERNANCE & ADMINISTRATION

Thank you for attending!