Cybersecurity Awareness

Stay ahead of cybersecurity threats

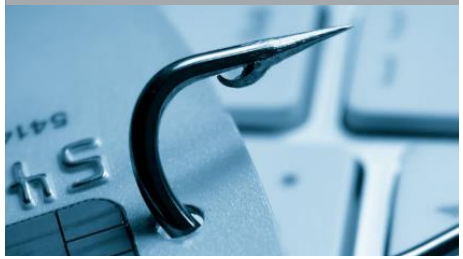
Jacob Lapacek

Treasury Management & Payments Consultant

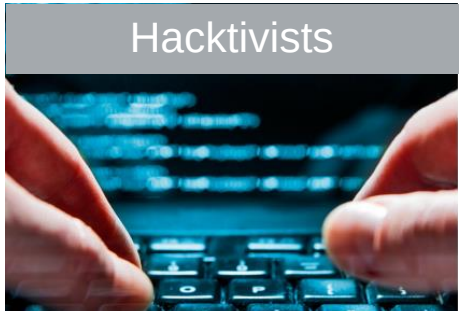
usbank

Rapidly evolving threats—motivational shifts

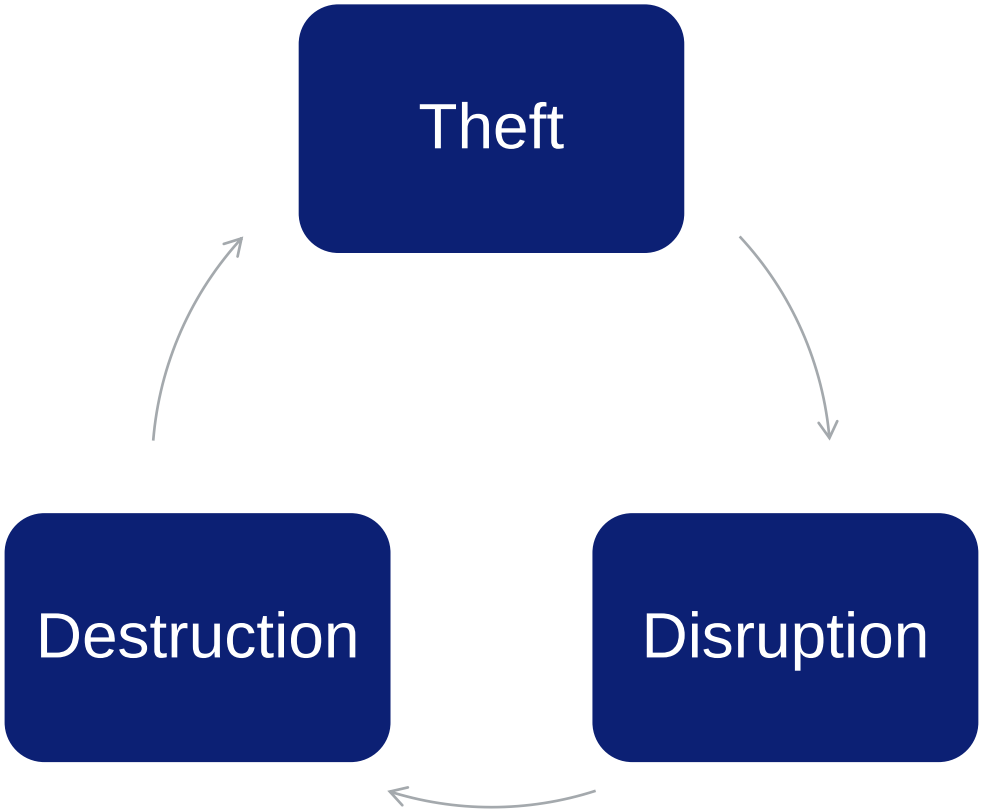
Fraudsters



Hacktivists



Nation-States



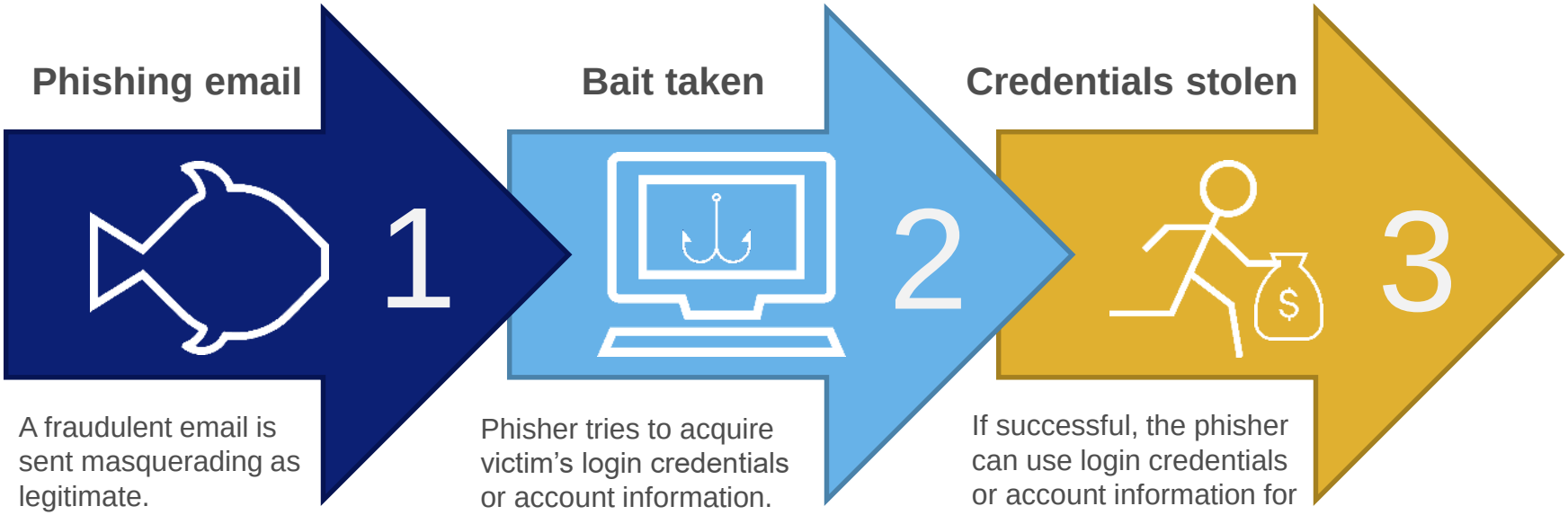
Cybersecurity alert: phishing

Things to look out for:

- “Phishy” company emails
- Requests for credentials or account information

Focused twists:

- “Spear phishing”
- Executives = “whales”
- Adding a telephone component



Know your risk

On average 85% of emails are stopped at the door

All industries are susceptible to clicking on a phishing message

One in 100 users will click on a phishing message

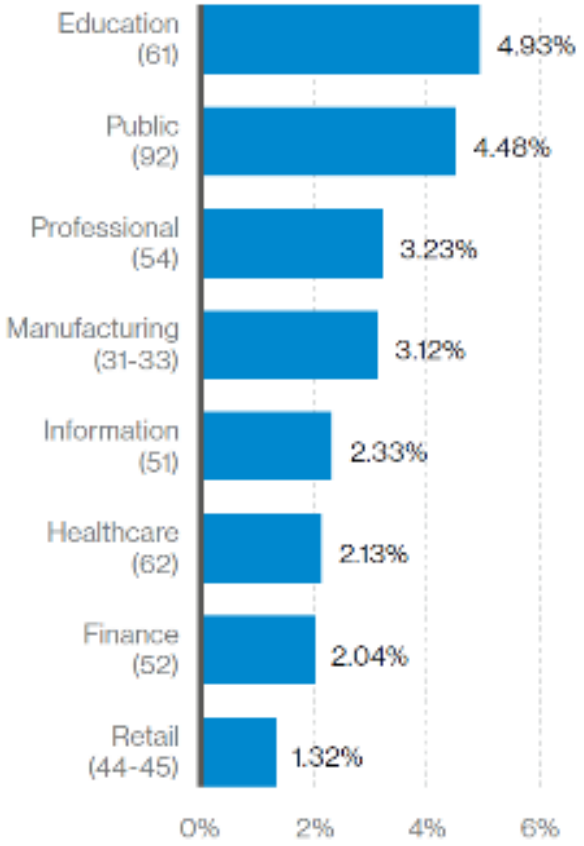
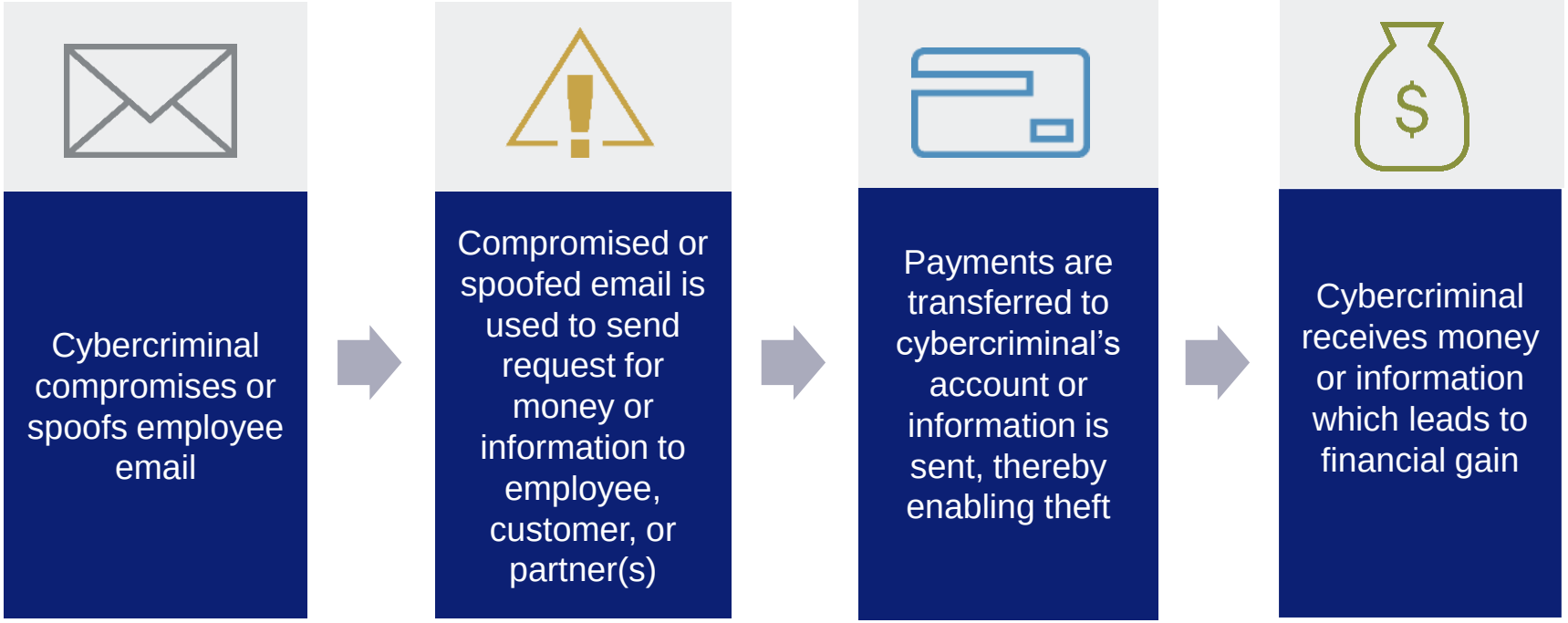


Figure 41. Click rate in phishing tests by industry

Source: https://enterprise.verizon.com/resources/reports/dbir/

Cybersecurity alert: business email compromise



"To sound legitimate, the attackers manipulate the tone of their email copy. They take on different personalities, including 'the authoritarian' who uses a direct and urgent approach, or 'the conversationalist' who builds a dialogue before asking for the request…" (Proofpoint 2017 Email Fraud Report)

Cybersecurity alert: business email compromise

Example of spoofed email

From: Sally.Smith@a**m**ycompany.com
To: Jeff Anderson
Subject: FWD: Payment to ABC Client

Jeff,

Need this processed immediately. Thanks.

Sally

---Begin Forwarded Message---
From: Bob.Jones@a**n**ycompany.com
Sent: Wednesday, April 16, 2015 3:40 PM
To: Sally.Smith@a**n**ycompany.com
Subject: Payment to ABC Client

Sally,

ABC Client called me personally this morning and is fairly upset at us. Need your team to complete the wire they asked for multiple times. Please transfer $151,023 from my admin to 12345678 acct 78910100 as soon as possible.

Bob

Pay attention to email domain names.
Here the attacker sent the email from "a**m**ycompany.com" and spoofed a previous internal email from "a**n**ycompany.com"

Business Email Compromise (BEC) is on the rise

$12B — **Total and potential losses globally since 2013** to BEC and Email Account Compromise

17% — **Increase in BEC attacks** last year

13 — Average **number of people targeted** in an organization

1/3rd — *Of BEC messages contain the word "payment" in the subject line;* ***Most attacks are designed with wire transfer fraud in mind)***

11% — *Of all email fraud attacks use* ***'fake email chain' messages****, to give a realistic experience and appear more credible*

Source: InfoSec Magazine - https://www.infosecurity-magazine.com/news/bec-attacks-jumped-17-last-year/

Cybersecurity alert: ransomware

From: DD4BC Team” <dd4bc@safe-mail.net>
Sent: Sunday, Feb 16, 2015 5:42 PM

Btw. Attack temporarily stopped. If payment not received within 6 hours, attack restarts and price will double up.

---Original Message---
From: “DD4BC Team” <dd4bc@safe-mail.net>
Sent: Sunday, Feb 16, 2015 12:34 PM
Subject: DDOS ATTACK!

Hello,

Your site is extremely vulnerable to DDoS attacks. I want to offer you info how to properly setup your protection, so that you can’t be ddosed. If you want infor on fixing it, pay me 1.5 BTC to 1E8R3cgnr2UcusyZ9k5KUvkj3fXYd9oWW6ABC

How malware and ransomware attacks work

1 Spear Phishing

An employee within the targeted organization receives an email with the malware.

2 Malware Stage 1

Upon opening the attachment, the malware is installed.

3 Malware Stage 2

The malware establishes communication to the attacker and downloads the program.

4 Victim Login

The program alters the bank's website, tricking the victim to call an illegitimate number.

5 Social Engineering

To overcome measures by the bank to protect against fraud, social engineers obtain critical information from the victim.

6 Money Transfer

Money is quickly and efficiently transferred from the victim's account to several offshore accounts.

7 DDoS

Immediately after the theft, a high volume DDoS against the victim starts, in order to distract or hinder investigation.

Source: http://securityintelligence.com/dyre-wolf/

Real-life examples of the largest cyber breaches

Payment card transaction company

- 134 million credit cards exposed
- Breach wasn't realized for nearly one year
- $145 million paid out to compensate for fraudulent payments

Credit bureau

- Personal information of 143 million consumers exposed
- 209K users' credit card info exposed

Online auction company

- 145 million users affected
- Names, addresses, DOBs, and passwords of all users exposed

Retailer

- Credit/debit card information and/or contact information of up to 110 million people compromised
- Cost of breach totals $162 million

Email provider

- 1.5 billion user accounts
- Largest data breach in history
- Breach cost company $350 million during acquisition talks

Source: CSO from IDG https://www.csoonline.com/article/2130877/data-breach/the-1

Understanding your cyber environment

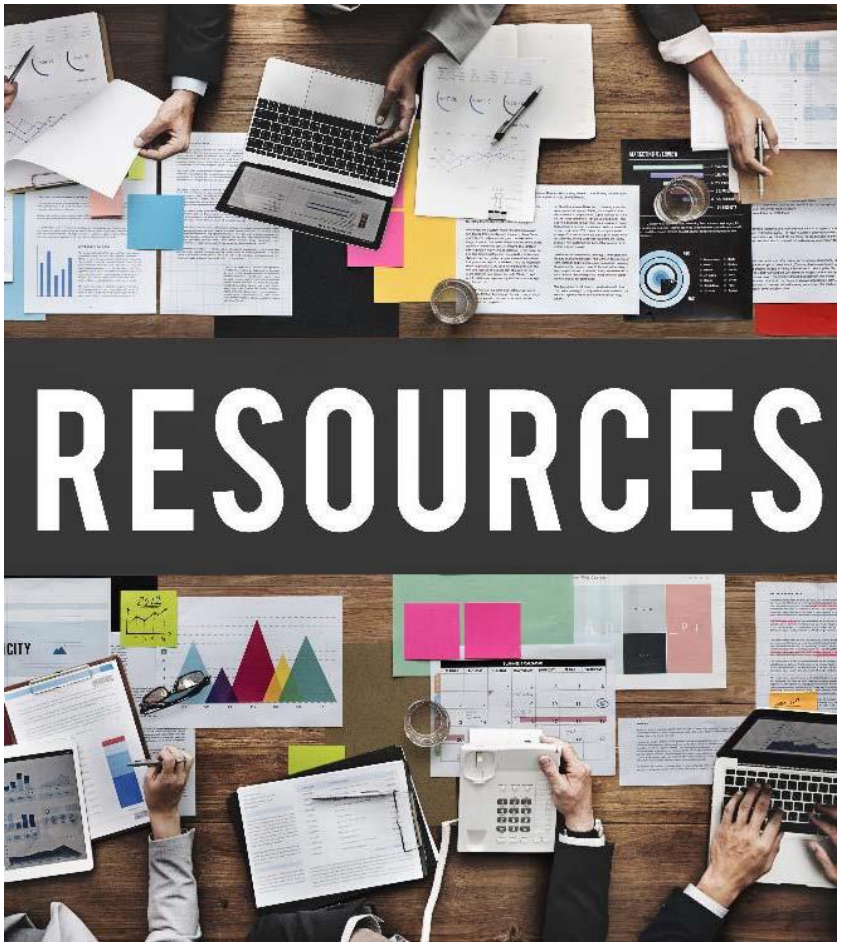
- What systems/data do you rely on most?
- Have you considered:
  - Confidentiality?
  - Integrity?
  - Availability?
- What cyber threats affect you?
- How are you vulnerable to them?
- How do you address cybersecurity risks?
- What gaps do you see?

Industry cybersecurity best practices

- Establish a sound governance framework
  - Consider the NIST Cybersecurity Framework
- Strengthen authentication/Dual Control
- Keep device software and antivirus “up-to-date”
- Back up sensitive data
- Develop & test incident response plans
- Communicate quickly
- Ongoing training, trust but verify
- Get engaged, create awareness

Report on Cybersecurity Practices, FINRA, February 2015
https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

Resources



Center for Internet Security
- Top 20 Controls https://www.cisecurity.org/controls/
- CIS Benchmarks (security hardening guidelines) https://www.cisecurity.org/cis-benchmarks/

Global Cyber Alliance
- Quad 9's DNS filter https://www.globalcyberalliance.org/quad9/
- DMARC Guide https://www.globalcyberalliance.org/dmarc/

SANS
- Security Awareness – Ouch Newsletter https://www.sans.org/security-awareness-training/ouch-newsletter

ISAC's
- Sector specific information sharing and analysis centers https://www.nationalisacs.org/

OWASP
- Best practices in application security https://www.owasp.org/index.php/Main_Page

Free resources

Partnerships & information sharing

- **National Defense Information Sharing and Analysis Center (ISAC)** – the national defense sector's information sharing and analysis center, offering a community and forum for cyber threat sharing: www.ndisac.org
- **InfraGard National Capital Region -** a partnership between the FBI and members of the private sector providing a vehicle for the timely exchange of information and promotes learning opportunities to protect Critical Infrastructure**:** www.infragardncr.org
- **Global Cyber Alliance -** working together to eradicate systemic cyber risk: www.globalcyberalliance.org
- **National Cybersecurity Awareness Month** - observed every October – a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online: www.staysafeonline.org/ncsam
- **STOP. THINK. CONNECT.** - global online safety awareness campaign to help all digital citizens stay safer and more secure online: www.stopthinkconnect.org

Government

- **NIST Cybersecurity Framework:** https://www.nist.gov/cyberframework
- **Federal Bureau of Investigation Cyber Division:** www.fbi.gov/investigate/cyber
- **Federal Trade Commission Privacy and Security Site:** https://www.ftc.gov/tips-advice/business-center/privacy-and-security

Free resources

U.S. Bank

- **Strength in Security annual cybersecurity conference** held in October during Cybersecurity Awareness Month. Stay tuned for 2019 details: www.strengthinsecurity.com
- **Financial IQ** – Strategies, inspiration, and thought leadership. Type “cyber” in search tool: www.financialiq.usbank.com
- **Online Security microsite** featuring various tips on how to stay safe in your personal and business life: https://www.usbank.com/online-security/

Publications

- **2018 Verizon Data Breach Investigations Report (2019 Report Coming Soon):** https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
- **Financial Services Information Security & Analysis Center - Destructive Malware Best Practices Paper:** https://www.fsisac.com/sites/default/files/news/Destructive%20Malware%20Paper%20TLP%20White%20VersionFINAL2.pdf
- **Ransomware Best Practices Paper:** https://www.uschamber.com/sites/default/files/documents/files/ransomware_e-version.pdf

Questions?