Cybersecurity Awareness Training

Mike Morris
Partner
404 420-5669
mike.morris@wipfli.com

Agenda

- What is cybersecurity
- Why are small business being targeted?
- Top hacking techniques
- How can you protect yourself?
- What is Auburn Bank doing to protect you?
- Q/A

What is cybersecurity?

- Proactively securing information assets and computers from disclosure from Internet-based hackers/fraudsters
- Demonstrating a strong security posture to deter or prevent potential cyber attackers (a.k.a. ‘hackers’ or ‘bad actors’)

Why Cybersecurity?

- We are at war (in cyberspace) and are losing (badly!)
- Countries are stealing billions of dollar from America each year
- Top 5 originating countries for U.S. targeted hacking attacks:
  - China
  - Brazil
  - Russia
  - Poland
  - Iran

Cybersecurity Risks

- Transactional – Money is stolen (money leaves your business)
- Reputational - “5:00 News”, loss of customer confidence
- Legal/Compliance – Customer lawsuits
- Operational – Your computers won’t work
- Strategic – Customer trust is broken so new products/services might suffer

Who are Our Adversaries

- We are up against opponents that are:
  - Highly skilled
  - Highly motivated
  - Well funded
  - Constantly looking for targets of opportunity regardless of size
  - Using advanced tools and skills

Who are Our Adversaries

- Professional hacking rings – run like a corporation
- State Sponsored Hackers
- Hacker can earn 16 times the median salary in their countries
- Over 65% of hackers spend 20 hours or less per week
- Difficult to find/extradite

Who are Our Adversaries

- Hacking is now a multibillion-dollar industry!

Small Business Hack Statistics 2024

- 46% of all cyber breaches impact businesses with fewer than 1,000 employees.
- 37% of companies hit by ransomware had fewer than 100 employees.
- Small businesses receive the highest rate of targeted malicious emails at one in 323

Small Business Hack Statistics 2024

- Employees of small businesses experience 350% more social engineering attacks than those at larger enterprises
- 27% of small businesses with no cybersecurity protections at all collect customers' credit card info
- Cybersecurity incidents at small to medium sized businesses cost between $826 and $653,587

Small Business Hack Statistics 2024

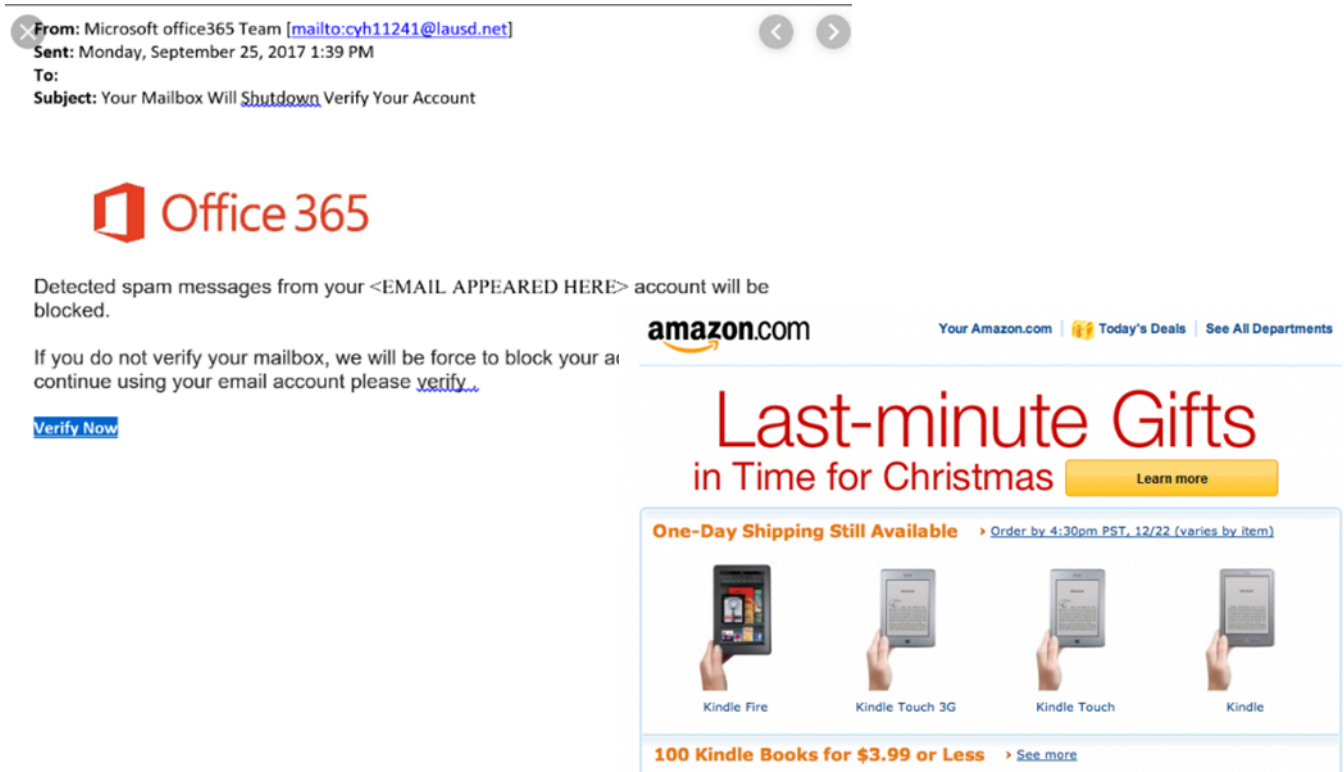
- Nearly 40% of small businesses reported they lost crucial data as a result of an attack
- 51% of small businesses that fall victim to ransomware pay the money
- Just 17% of small businesses have cyber insurance

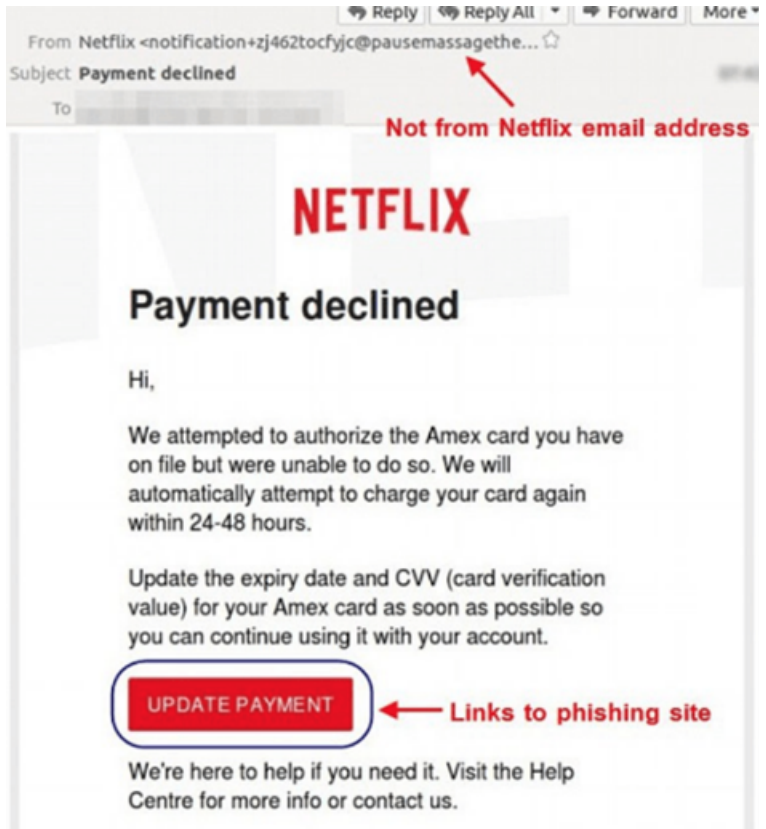
Top Attacks

- Phishing
- Business Email Compromise (BEC)
- Corporate Account Takeovers
- Ransomware
- Malware
- Drive-by Downloads/Waterholes (Web Surfing)

Phishing

- Hackers send out mass spam emails (or targeted emails) to get users to take the bait:





Phishing

- 90%+ of reported hacks have started through phishing attacks against employees (it only takes one)!
- Notable 2024 attacks that started with phishing:

Phishing Example

Subject: Investment Profile

From: Tim@safenet34.io

Reply-To:Tim@mysafenet2.com

To: casey.flanagan@zwjic.com; mike.klm@klm.com sandral@invest.com;

Date: Thursday, September 1, 2:30am

Investmentinfo.exe

The attached file is my portfolio information. Please open and review the information before the end of the business day. I will be traveling and need your response today.

Variants - Spear Phishing and Whaling

- Phishing = they don’t necessarily know who you are
- Spear Phishing = They have identified you as a target
- Whaling = targeting high-value targets link business owners and executives

Phishing Attacks – Tips to Protect Yourself

Red flags:

- There is a threat (account will be deleted, you will go to jail, you will be fined, you will be fired)
- There is an emergency (“this wire must be sent immediately or our customer will be upset!”)
- The sender is unavailable (“I need this done by 5:00 but I am in a meeting and can’t check email or take calls!”)

Phishing Attacks – Tips to Protect Yourself

Red flags:

- The email is from an unknown sender or the email address structure/domain is not right
  - mike@auburnbank.com

    versus:
  - mike@auburmbank.com
- There is a free coupon for a popular brand
- Improper grammar/odd way of saying things

Phishing Attacks – Tips to Protect Yourself

- Do not click on hyperlinks – open a browser and go to the website directly
- Be wary of attachments
- When in doubt, call the sender
- Report senders: “Report Spam”

Phishing Attacks – Tips to Protect Yourself

- Configure you email system filters (these are rules to block certain types of emails from being allowed to hit a user's inbox)
  - Example: Block all inbound emails with your domain that originate outside of your organization (a.k.a. "Spoofing"

- Train your employees

Vishing

- Hackers use the telephone to trick people into providing sensitive information
- Deep fakes can be used to sound like known people.
- Deep fakes = using real peoples voices and images to create fake requests

Smishing (SMS Phishing)

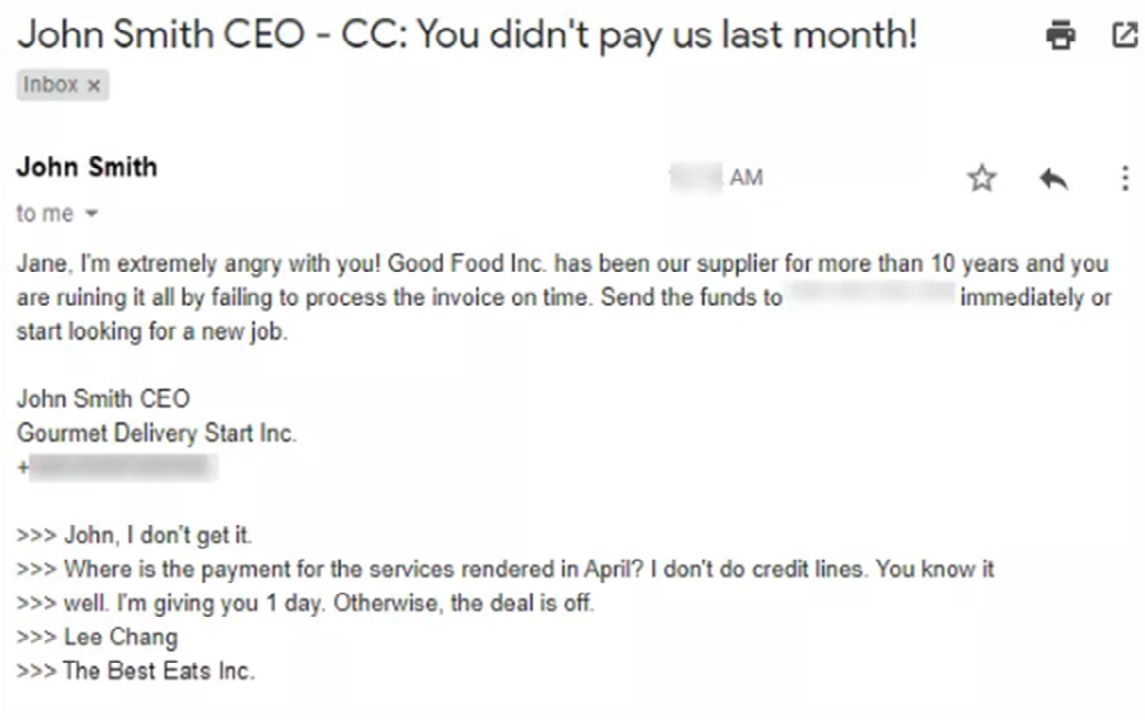
- Hackers use text messaging or messaging apps (WhatsApp) to trick people into providing personal information or clicking on malicious links
- Popular because people are more likely to click on links in text messages
- Smishing attacks can include
  - Package tracking scams
  - Service cancellation
  - Job offers

Smishing (SMS Phishing) – Tips to Protect Yourself

- Don’t respond if you don’t recognize the name or number
- Never provide any information to an unknown number
- Consider blocking the number to prevent future attacks from that user

Business Email Compromise (BEC)

- BEC involves spoofed emails that look like they’re coming from a trusted source such as:
  - Company executive
  - Employee
  - Vendor
- In 2023 the FBI estimated BEC-related losses totaled nearly $2.9 billion


John Smith CEO - CC: You didn't pay us last month!

Inbox ×

John Smith [redacted] AM

to me

Jane, I'm extremely angry with you! Good Food Inc. has been our supplier for more than 10 years and you are ruining it all by failing to process the invoice on time. Send the funds to [redacted] immediately or start looking for a new job.

John Smith CEO
Gourmet Delivery Start Inc.
+[redacted]

>>> John, I don't get it.
>>> Where is the payment for the services rendered in April? I don't do credit lines. You know it
>>> well. I'm giving you 1 day. Otherwise, the deal is off.
>>> Lee Chang
>>> The Best Eats Inc.

Business Email Compromise (BEC) – Tips to Protect Yourself

- Be wary of email requests that are requesting money
- Call the person from a number that is known/published (not the one in the suspicious email)
- Follow the standard red flags from the phishing attack tips

Corporate Account Takeover

- Hackers gain access to a company's bank accounts, social media sites, websites, accounts payable systems, etc.
- Once they have access, they move money out of the accounts through wires, bill pay, or ACH

Malware/Advanced Persistent Threats

- You can be infected through phishing, web surfing, checking personal email on work computers, bringing in removable storage devices from home, etc.
- Hackers are usually trying to get an internal foothold
- The malware installed and the people involved (hackers) are called Advanced Persistent Threats “APTs”
- Once inside they will use tools to monitor and control network resources

Malware/Advanced Persistent Threats

- The heart of these tools is typically a keystroke logger and Command and Control (C&C) software
- Once inside, the hackers typically place multiple tools and backdoors so that if one fails or is identified and removed, they have another way in
- They are getting these tools installed by end users through phishing or waterhole attacks

Web Surfing Risks

- Hackers use both fake and legitimate (compromised) websites to infect users surfing these sites

Top Ten on McAfee's Hacker Celebrity Hot List

The top ten list, which includes a combination of longtime talent and more recently well-known names, is as follows:

1. **Ryan Gosling**, critically acclaimed actor and star of this summer's hit film, Barbie.
2. **Emily Blunt**, critically acclaimed actress and star of this summer's hit film, Oppenheimer
3. **Jennifer Lopez**, pop culture icon, critically acclaimed singer, actress and producer
4. **Zendaya**, critically acclaimed actress and singer
5. **Kevin Costner**, critically acclaimed actor and director, and star of the hit series, Yellowstone
6. **Elon Musk**, business magnate and tech entrepreneur
7. **Al Roker**, TODAY's weather man, author, and journalist
8. **Margot Robbie**, critically acclaimed actress and star of this summer's hit film, Barbie
9. **Bad Bunny**, critically acclaimed singer, and the first non-English language singer to be named as Spotify's most streamed artist of the year
10. **America Ferrera**, critically acclaimed actress and noted supporting star of this summer's hit film, Barbie

- Don't visit non-business related websites on Bank-owned computers (and be careful at home!)
- Don't click on hyperlinks in email, go directly to the legit site

Web Surfing Risks

- Watering Hole Attacks
  - Hackers seek to compromise a specific group of end users by infecting websites that members of the group are known to visit.

Web Surfing Risks

- Drive-by Downloads
  - Legitimate site have ads that contain malware.
  - If your browser (or supporting software – Adobe, Java, etc.) is out of date, they can install onto your computer automatically

Emerging Risks – Deep Fakes

- Hackers are using AI to create very realistic deep fakes
- A client recently got hit with a deep fake (voice only) of their CEO
- The hackers were trying to get employees to wire money

CEO 'Deep Fake' Swindles Company Out of $243K

Emerging Risks – Deep Fakes

- Same red flags as BEC
  - Urgent request
  - Wires that need to be sent to a new account

- Also consider:
  - Behavior that is not in line with the known person
  - Phrasing of speech
  - When in doubt - contact the person

Paper Documents

- Protect paper documents – shred all sensitive information
- Dumpster diving – if documents make it to the dumpster, it is easy to compromise!
- Don’t write down your passwords

Auburn Bank Controls to Protect You

- Multifactor Authentication
- Encryption
- Positive Pay
- Dual Control
- Exposure Limits

Questions

Michael Morris, CISA, CISSP

mike.morris@wipfli.com
404.420.5669