Staying Safe Online

Montpelier Senior Center

Week #1 – Mon 5 Jan 2026

Protecting Against Fraud (Part 1)

M. E. Kabay, PhD
Emeritus Professor – BSc & MSc Cybersecurity Programs
Norwich University

https://tinyurl.com/3b6p3h8s

1

1

Topics

- Spam
  - Unsolicited email
- Phishing
  - Tricking victims into revealing info or downloading malware
- Trojans
  - Malware downloads
- Advance-fee fraud
- Refund scams
- Blackmail

2

2

What is Spam?

- Unsolicited email
  - Recipient never asked for or permitted emails from the sender
  - Estimated volume:
    - ✓160 billion spam emails per DAY worldwide
    - ✓~46% of world total of 347 billion emails/day
- Fraud rampant in spam
  - ~600 million victims worldwide/year
  - Losses ~$1 trillion worldwide/year
- Dangers
  - Cluttering inbox – can lose track of legitimate email
  - Naïve recipients click on links – harmful materials
  - False identification tricks victims into thinking they are responding to legitimate services (government, technical support, software licenses….)

3

3

Origins of the Term "spam"

- Monty Python 1970 – The Spam Sketch

https://tinyurl.com/4r55f7ry

[Hormel Corporation politely requests that their food-like product be referred to as "SPAM."]

4

4

The US CAN-SPAM Act

- CAN-SPAM Act of 2003 [15 U.S.C. § 7704(a)]
- Accurate header showing origin of email
- Non-deceptive subject line
- Clear indication of advertisement or fund-raising
- Working return e-mail address
- Easy opt-out link to work within 10 days
- No further spam after opt-out
- Valid physical postal address for sender
- Penalties can include
  - Fines up to $250 per email
  - Penalties up to U$2 million
  - Possible imprisonment
- May report abuse to Federal Trade Commission
  - https://reportfraud.ftc.gov/

5

5

Phishing (1)

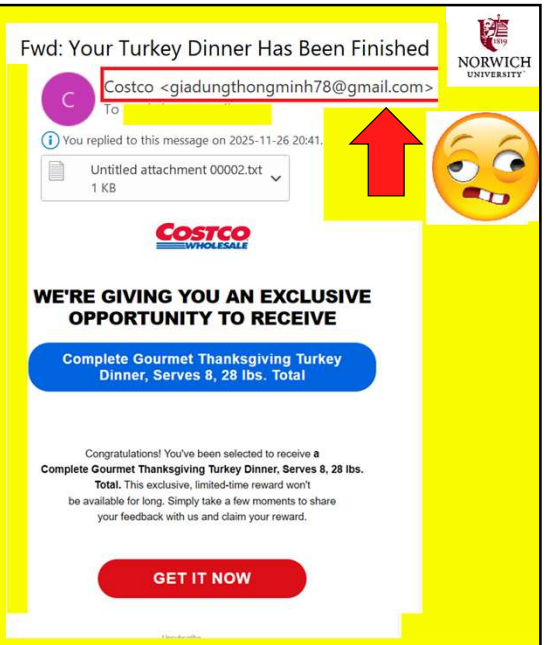
- Goal: obtain personal information for further fraud
- Methods
  - Fake websites (imitating real ones)
  - Tricking victims into revealing secret info
    - ✓ User ID (e.g., email, banks, gov't sites
    - ✓ Passwords
    - ✓ Social-Security ID
    - ✓ Bank info
- KEY POINT: ALWAYS HOVER POINTER OVER A LINK TO SEE WHERE IT IS GOING! If link for your bank goes to a Russian (.ru) site, IT ISN'T REAL!!!
- *Up-to-date* established antimalware products; e.g., (not an exclusive list)
  - BitDefender
  - Norton AntiVirus
  - Windows Defender
  - McAfee Antivirus

6

6

Phishing (2)

- Check the origination address of ALL emails, especially those claiming to be from a company.
- DO NOT OPEN ATTACHMENTS
- The real example here is from an idiot who used GMAIL!! LOL!



7

7

Advance-fee Fraud

- AKA "Nigerian 419 Scam"
- Criminals announce huge payment (often $millions)
  - "Government payment"
  - "Legal payment from class-action lawsuit"
  - Nonexistent "lottery winning" (without participation!)
  - "Donation from a dying millionaire" (often a "widow")
- Victims supply detailed info
  - Name, address, phone number, bank account (!)
- Criminals request payment (e.g., $150) through a commercial cash card
  - Walgreens
  - Staples
  - Amazon
  - Etc.
- Steal the money

8

8

Refund Scams

- Emails or phone calls about non-existent payments
  - Caller or email pretend to be from a company
  - Often send millions of messages
    - ✓ May have nothing to do with potential victims' actual software or purchases
- E.g., Email or phone message
  - "You have been billed $429 for one year of your McAfee antivirus" (which the victim does not use)
  - "If this information is wrong, phone XXX-XXX-XXXX
- Criminal apologizes & asks to access bank account
  - Victim (e.g., my 90-year-old aunt) agrees to let criminal install remote-access software to "see bank account"
  - Steals details of banking account & logon & password
- Pretends to refund 10x fake amount & whines about it
- Victim authorizes wire transfer for non-existent payment
- *I stopped the theft of $30,000 from aunt's account!*

 9

9

Threats of Prosecution

- "FBI" or "State Police" or "IRS"
  - Email with phone number to call
  - Phone call with threats from "official"
  - Text message with link or phone # to call
- "You are being charged with XYZ crime"
  - "Must pay $ (often thousands) to avoid prosecution"
- That's not how law-enforcement works!
  - LEO do not warn suspects of arrest!
  - Justice system does not ask for money to avoid trials!
- Block the emails and block phone calls from #
- Swear at the phone callers & hang up

 10

10

Blackmail

- Typical script by email or phone:
  - "I've been watching you for a month using a virus I installed on your computer."
  - "I have recorded you doing {bad things list}"
  - "Unless you pay me {large amount of money} I will post the videos online and arrange {bad consequences}"
- Typically threats involve something sexual
- But what kind of idiot pays a criminal NOT to do something?
- What could possibly stop an endless series of demands??

11

11

Unwanted Phone Calls

- Our phone #s can be widely distributed
- US established DO NOT CALL (DNC) LIST
  - Irresponsible companies and criminals have been collecting those DNC #s for spam calls
- Install inexpensive call-blocking software; e.g.,
  - Android: Should I Answer?
  - Apple iOS: Robokillerheaders
- These products share info from users
  - Can update manually or automatically
  - Work well!

12

12

Advice Summary

- Install established anti-malware products on computers and phones
- Never click on an unfamiliar link on Web or in Email without seeing where it is *actually* going online
- Don't respond to unexpected emails or phone calls
  - Look up the *real* contact info yourself
- Never let a caller install software to control your system
- Never agree to let anyone "deposit money" to your bank account
- Never agree to pay money for a gift or prize
- Never respond to email, text or phone threats
- Never respond to online claims that a government agency is going to fine you or send you to jail
- Never respond to supposed blackmail threats

13

13

OK, STAY SAFE!

14

14