Unlocking the Secrets of Telephone Phreaking

Phreaking and its implications on modern cyber threats

AGENDA

- Who am I?
- What is Phreaking?
- Telephony
  - POTS vs VoIP
- Phreaking History
  - Evolution
  - Significance
- Classic Phreaking tools and techniques
- Emerging threats in telephony
  - Risks and consequences
  - Mitigation and best practices
  - Proactive defense

Who Am I?

- Co-Founder of the PhilTel project, aiming to install free-to-use payphones within Philadelphia
- Run the Philly 2600 hacking meetups
- Not in InfoSec
  - Software Engineer
  - Views expressed here are my own, not those of my employer
- Fascinated by hacker/phreaker culture and history

“PHREAKING”

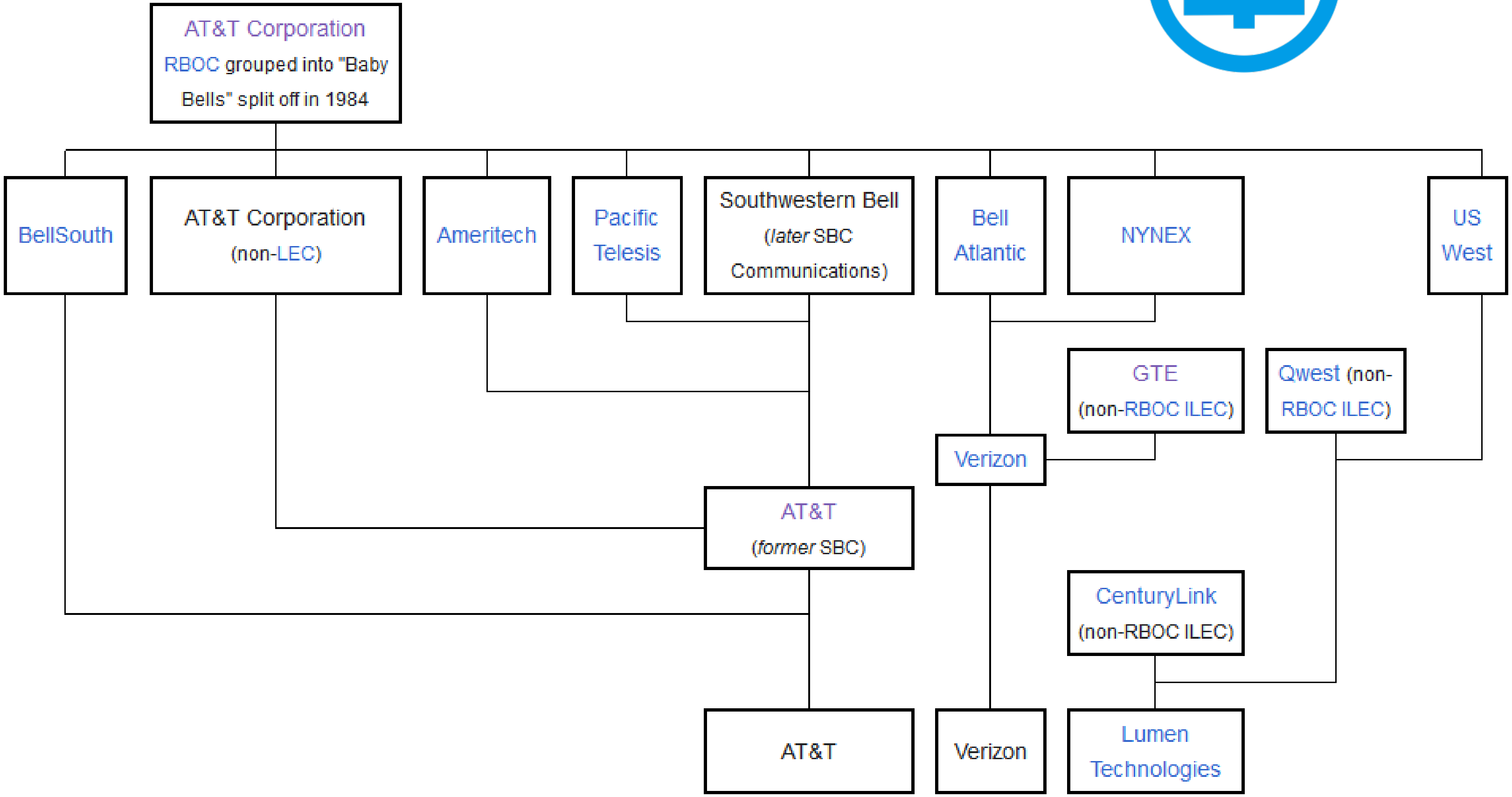
- A slang term coined to describe the activity of a culture of people who study, experiment with, or explore telecommunication systems, such as equipment and systems connected to public telephone networks
- Phreaking is not always about toll fraud or malicious activities

Telephony

TELEPHONY

TELEPHONY

“The Phone Company”



AT&T Corporation RBOC grouped into "Baby Bells" split off in 1984

BellSouth

AT&T Corporation (non-LEC)

Ameritech

Pacific Telesis

Southwestern Bell (*later* SBC Communications)

Bell Atlantic

NYNEX

US West

GTE (non-RBOC ILEC)

Qwest (non-RBOC ILEC)

Verizon

AT&T (*former* SBC)

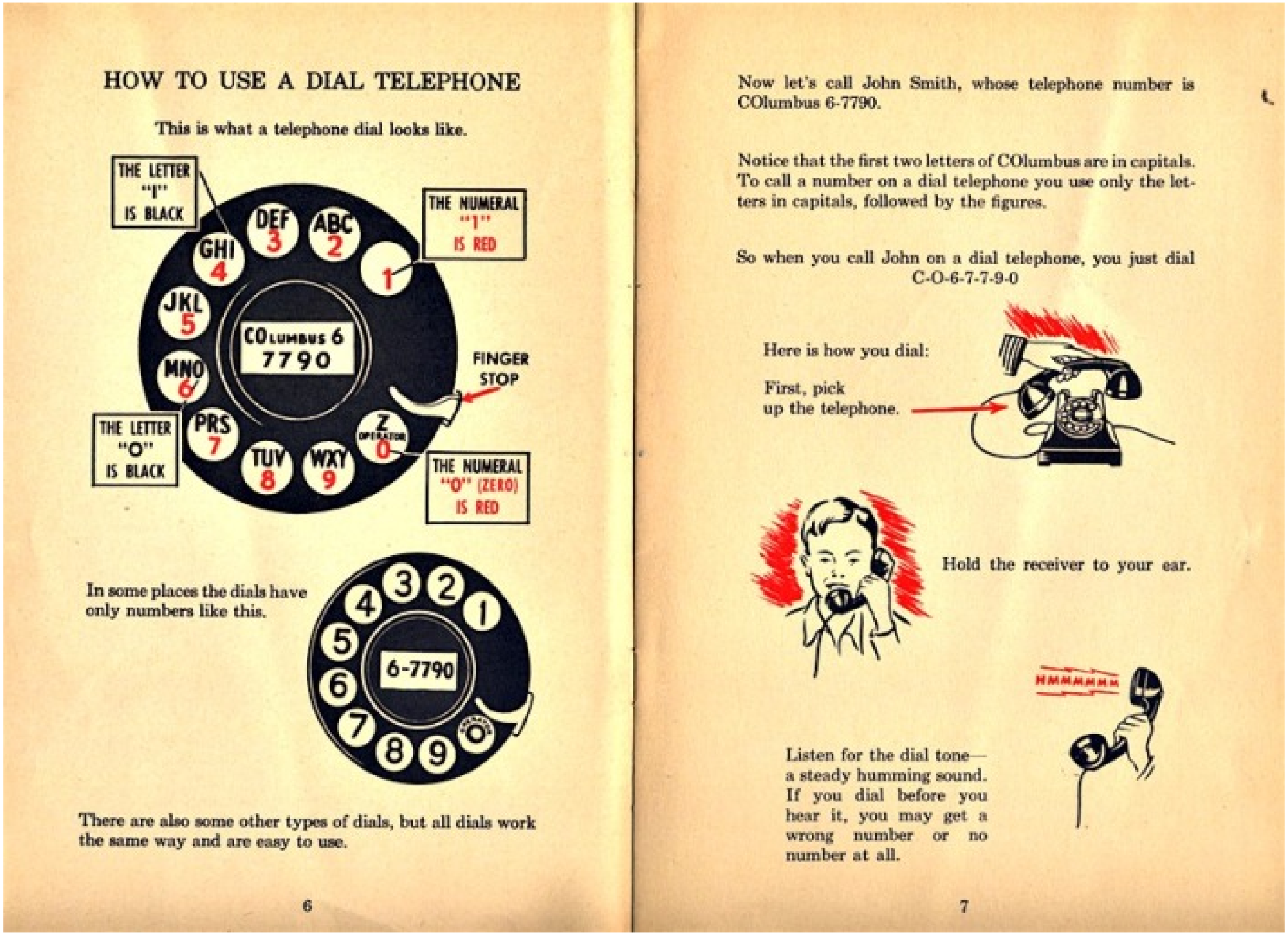
CenturyLink (non-RBOC ILEC)

AT&T

Verizon

Lumen Technologies

Telephone Numbers



HOW TO USE A DIAL TELEPHONE

This is what a telephone dial looks like.

THE LETTER "I" IS BLACK
THE NUMERAL "1" IS RED
DEF 3
ABC 2
GHI 4
1
JKL 5
COLUMBUS 6 7790
MNO 6
FINGER STOP
PRS 7
TUV 8
WXY 9
Z OPERATOR 0
THE LETTER "O" IS BLACK
THE NUMERAL "0" (ZERO) IS RED

In some places the dials have only numbers like this.

3
2
4
1
5
6-7790
6
7
8
9
OPERATOR 0

There are also some other types of dials, but all dials work the same way and are easy to use.

6

Now let's call John Smith, whose telephone number is COlumbus 6-7790.

Notice that the first two letters of COlumbus are in capitals. To call a number on a dial telephone you use only the letters in capitals, followed by the figures.

So when you call John on a dial telephone, you just dial C-O-6-7-7-9-0

Here is how you dial:

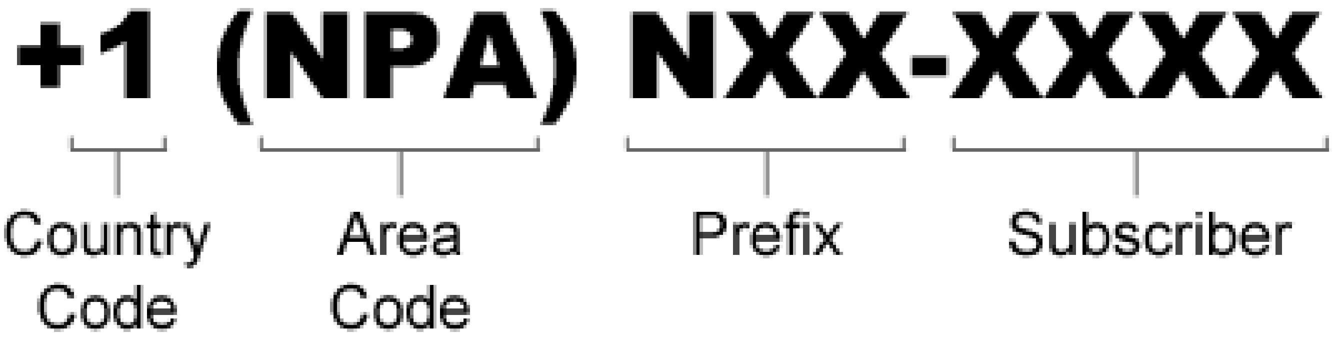
First, pick up the telephone.

Hold the receiver to your ear.

Listen for the dial tone—a steady humming sound. If you dial before you hear it, you may get a wrong number or no number at all.

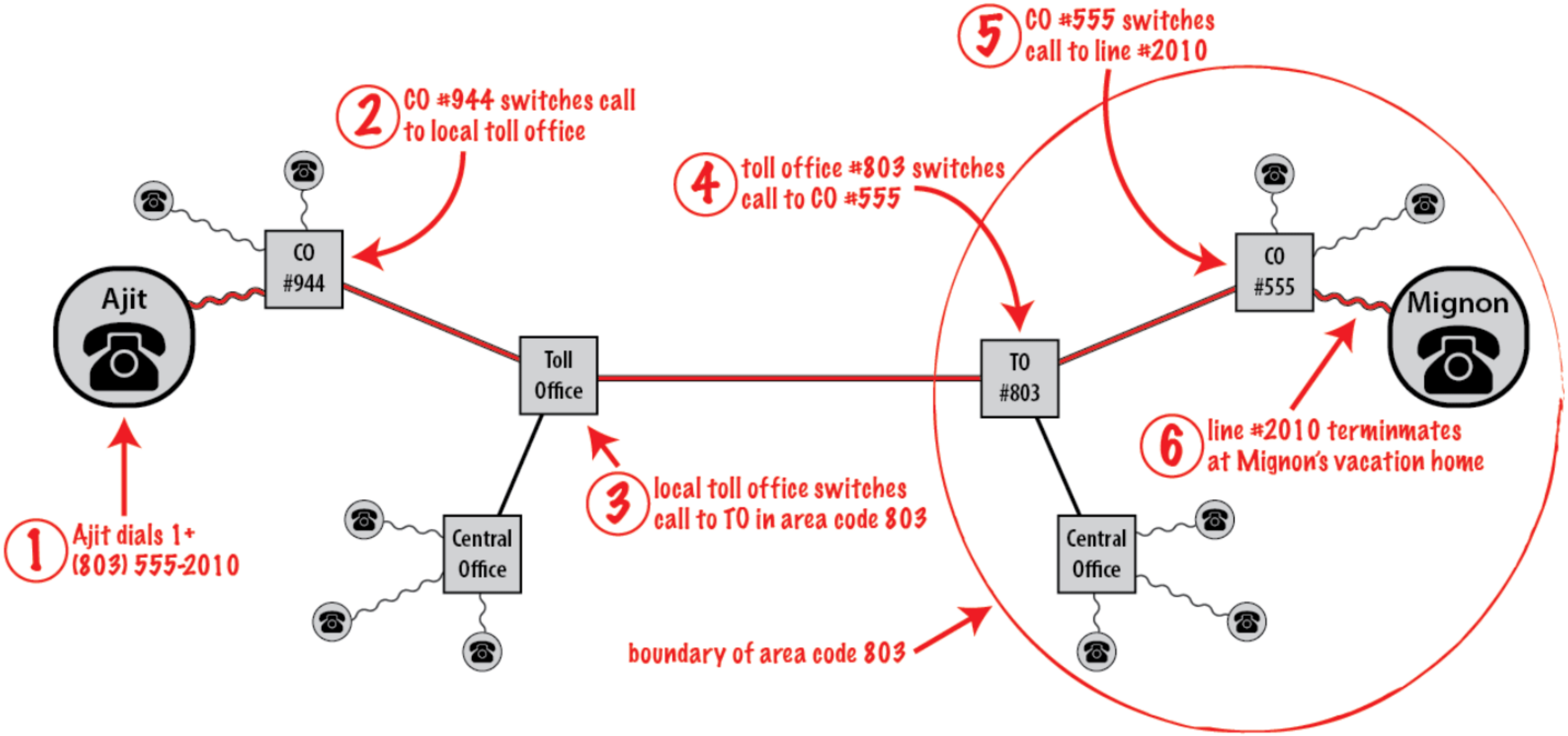
7

Telephone Numbers



- NPA = Number Plan Area

Analog/Digital Telephony (POTS)

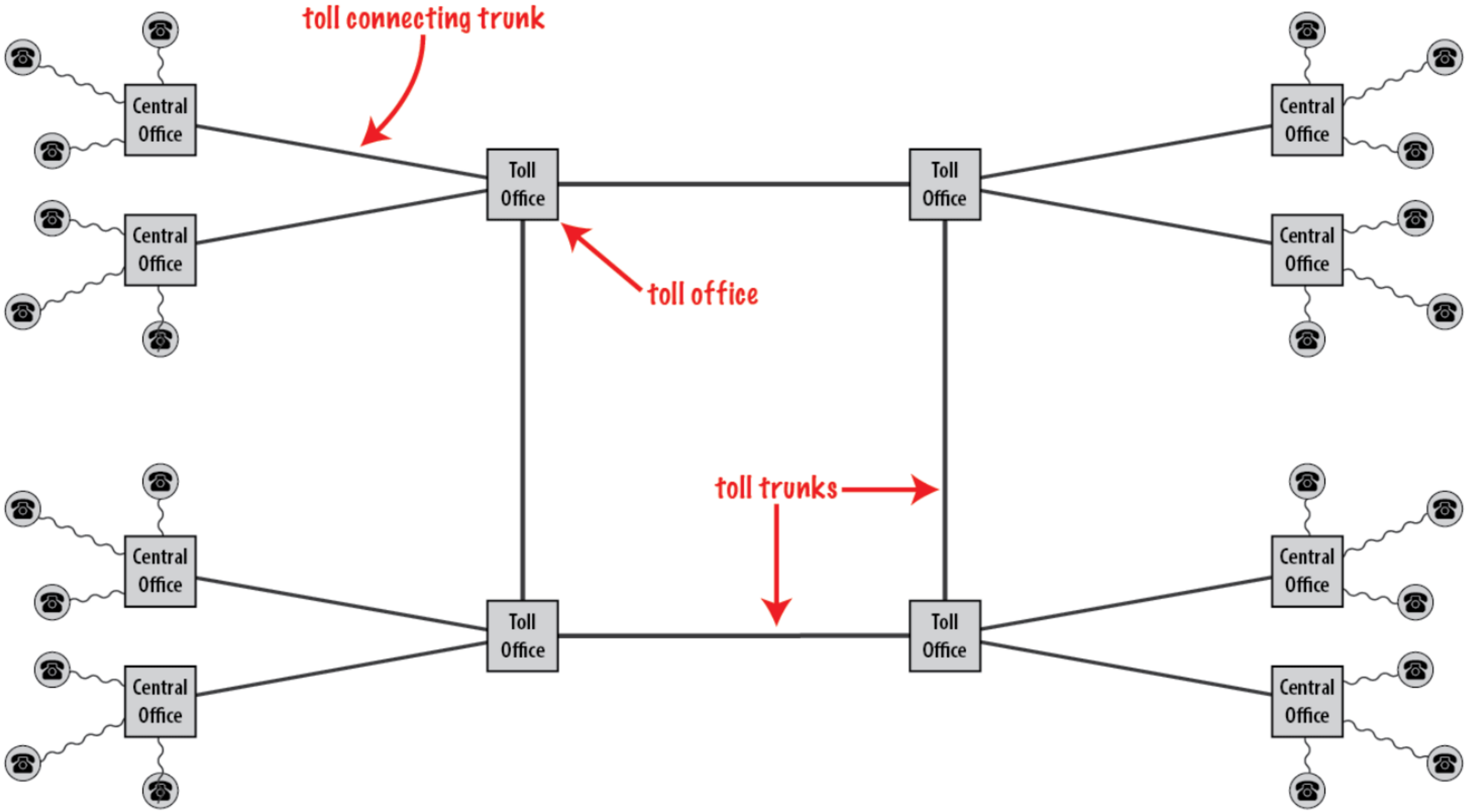


CO #555 switches call to line #2010
5
CO #944 switches call to local toll office
2
toll office #803 switches call to CO #555
4
CO #944
Ajit
Toll Office
TO #803
CO #555
Mignon
line #2010 terminmates at Mignon's vacation home
6
local toll office switches call to TO in area code 803
3
Ajit dials 1+ (803) 555-2010
1
Central Office
Central Office
boundary of area code 803

ANALOG/DIGITAL TELEPHONY (POTS)

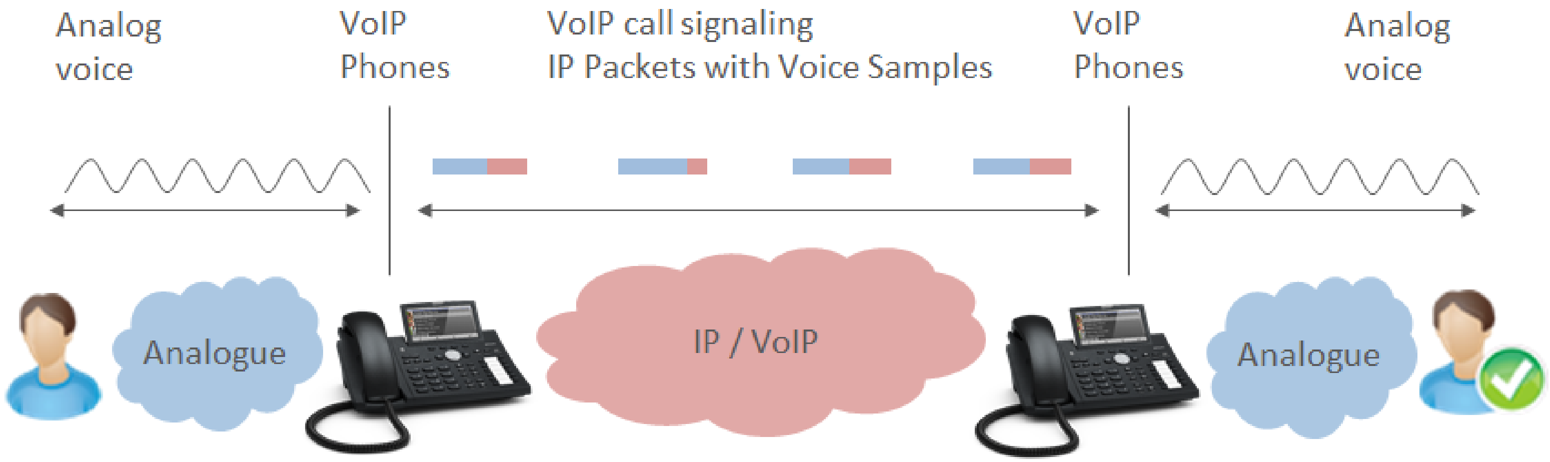
- Central Office
  - Exchange
- Local Loop (Subscriber line)
  - Literally a direct circuit between two phones
- Circuit-Switched
  - Physical path dedicated to one connection
- Controlled by big Telcos

Analog Telephony (POTS)



IP Telephony (VoIP)

- Voice-over-Internet-Protocol
- Telephony over the Internet
- Packet-Switched
  - Not a dedicated physical medium
- Inexpensive



Phreaking History

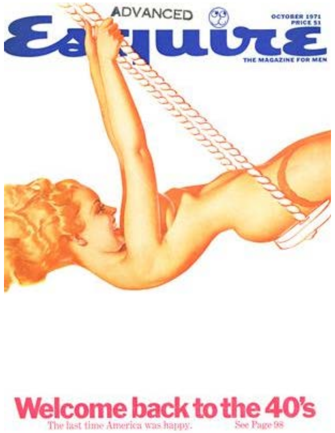
- Joybubbles discovered he could "hook-flash" a phone to dial numbers. Later, he discovered he had perfect pitch and could shut off telephone messages and place calls by whistling at 2600Hz

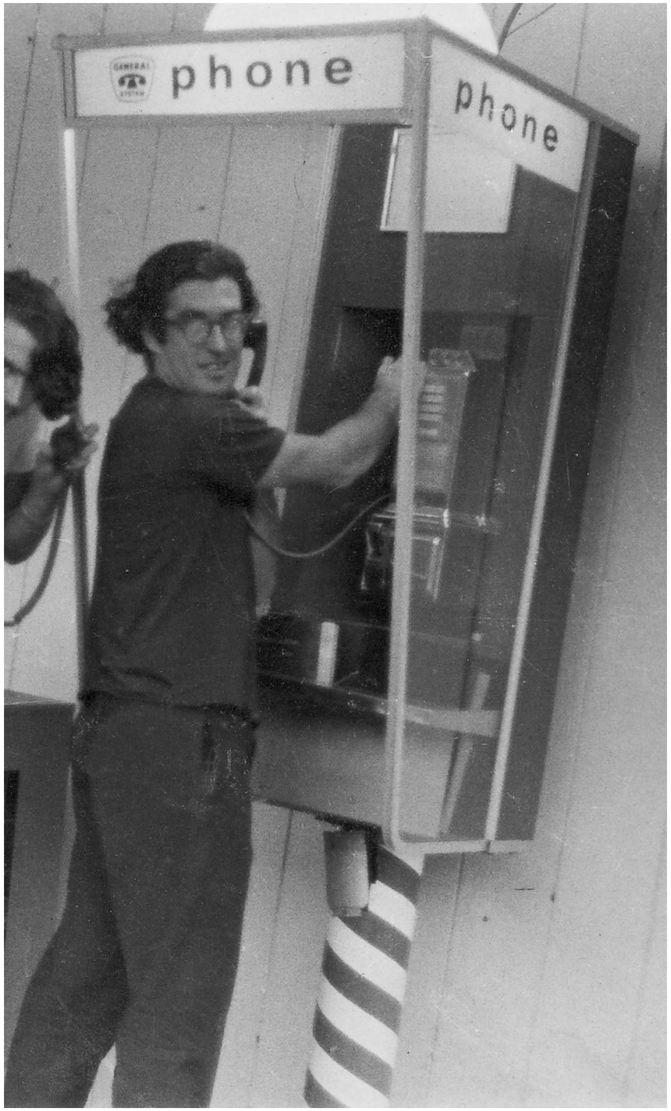
PHREAKING HISTORY

- Captain Crunch (John Draper), discovered a Cap'n Crunch Bo'sun whistle given as a toy in cereal boxes could produce that same 2600Hz tone.

Phreaking History

- Crunch was an early user and builder of Blue Boxes (used for making free long distance calls) and was featured in the 1971 *Esquire* article “Secrets of the Little Blue Box” with Joybubbles





Phreaking History

- Phreaking exploded in popularity, inspiring a whole generation to tinker with the phone network
- Phreaks had their own magazines/newsletters (TAP, 2600), phreaking was seen in movies (WarGames), contributing to the ‘70s/’80s zeitgeist

Phreaking Evolution

- Phreaks were constantly playing a cat and mouse game with Bell (and its descendants)
- While more attention was drawn to phreaking, toll fraud increased, giving phreaking a bad name
- Eventually, phone companies would patch their security holes and render techniques obsolete
- More modern malicious phreaking targets Private Branch Exchanges (PBXs) owned by individuals/businesses
- There are still people exploring the phone network, especially focusing on more traditional elements, like circuit switching, payphones, etc.

Phreaking Significance

- Modern hacking/InfoSec movements can trace its roots back to phreaking
- With the advent of personal computing in the 1980s, many curious and tech-savvy people would communicate over bulletin board systems to share information about exploring the phone system and, increasingly, the computers that were connected to it

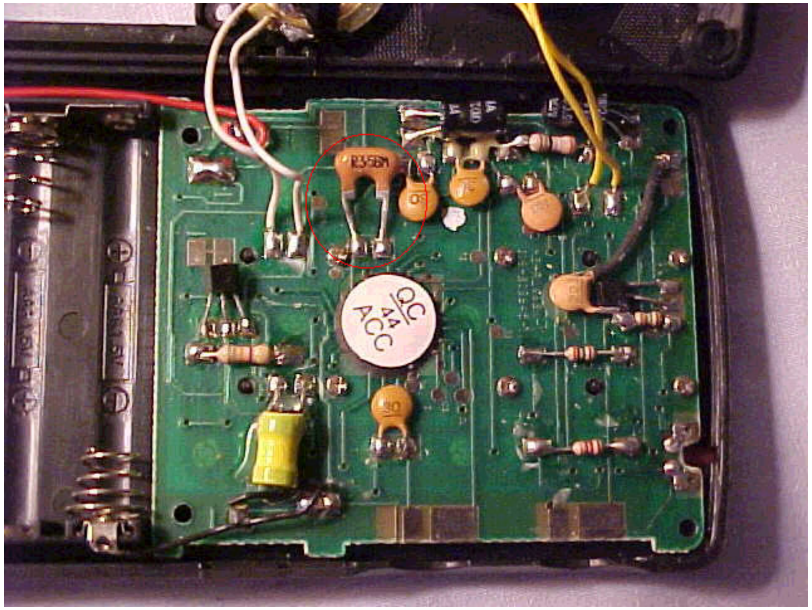
```
                WELCOME TO
              DURA-EUROPOS
        Built with GBBS Pro BBS software.
        Originally on-line from 1986-1993.
Resurrected from backup disks and placed on the internet in 2016.

   Other Sites   Apple II: bbs.impakt.net:6502
                 Apple II: sanctumbbs.com:[illegible]
               Atari [illegible]: bbs.[illegible]bbs.org:[illegible]
            Commodore 128: particlesbbs.dyndns.org:6400
(Enter [illegible] for a quick look around.)
Enter your ID#, HANDLE, NEW or '?':_
```

PHREAKING TOOL: BLUE BOX

- Exploited In-band Signaling (like SS5)
- Early blue boxes were single-frequency (SF) only, sending 2600Hz in different lengths and quantities to setup a call
- Later blue boxes utilized multi-frequency (MF) tones

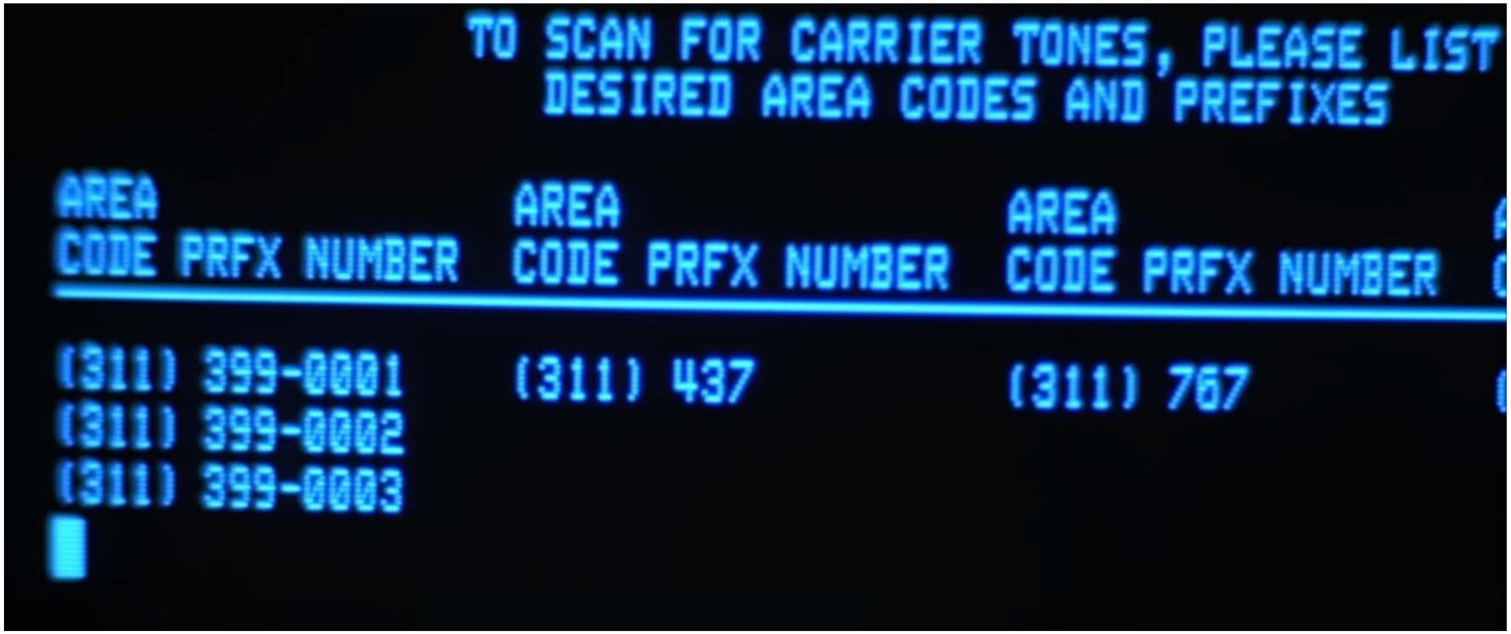
Phreaking Tool: Red Box

- Mimicked a nickel tone generated by a payphone to report that a coin had been inserted. Larger coins play the same tone multiple times
- Radio Shack tone dialers were often modified with a 6.5536 MHz crystal, allowing the user to press the * key to generate the coin tone



PHREAKING TECHNIQUE: WAR DIALING

- Using automated software to scan a range of telephone numbers to look for modems, computers, and other systems connected to the phone line
- Often combined with Calling Card Fraud
  - Call long distance provider, try card digits, dial a modem



```
                    TO SCAN FOR CARRIER TONES, PLEASE LIST
                       DESIRED AREA CODES AND PREFIXES

AREA                   AREA                   AREA
CODE PRFX NUMBER       CODE PRFX NUMBER       CODE PRFX NUMBER
-------------------------------------------------------------------
(311) 399-0001         (311) 437              (311) 767
(311) 399-0002
(311) 399-0003
```

Phreaking Technique: Social Engineering

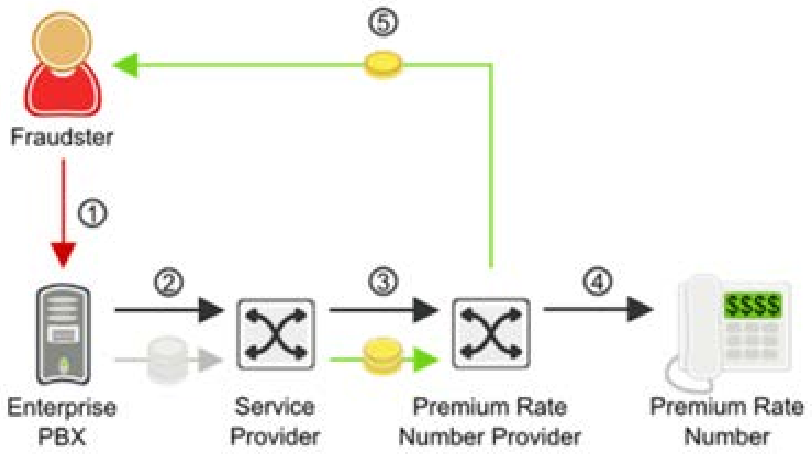
- Talking a target into revealing specific information or performing a specific action for illegitimate reasons
- Phreaks would social engineer telephone operators pretending to be Telco personnel
- Social Engineering is still prominent today. Hackers breached MGM last year by impersonating an employee in a voice social engineering attack that targeted the company's help desk (RN)

Emerging Threat: Caller ID Spoofing, Vishing

- An attack that causes a target's phone to display a phone number different than the one originating a call
  - This is actually a legitimate feature, used illegitimately!
- Vishing often utilizes caller ID spoofing to get sensitive information from targets
- Case Study: iSpoof (2002)
  - Targeted 142 people in Europe
  - 10 million fraudulent calls
  - Posed as bank personnel
  - Scammed $121 million

Emerging Threat: PBX Hacking

- Many modern Voice-over-IP systems can be setup quickly with default or poorly configured options
  - Default password for account, allow call forwarding
- Attackers can then use these systems to call toll numbers they own which charges the owner of the phone system
- Case study: Noor Aziz Uddin (2015)
  - Active 2008-2012
  - Grossed $50 million



Risks and Consequences

- While VoIP can be inexpensive and easy to use, it is rife with fraud and hacking
- Targets could divulge sensitive information or have their own systems hijacked to drive up a large phone bill
- Phone systems are just as vulnerable and exploitable as computers, and they often ARE just normal computers
- Phones also connect to the Internet and provide an entry point into your environment. People underestimate the risk of phone systems. Printers as well (RN)

Mitigation Strategies & Best Practices

- If someone calling you on the phone doesn’t seem quite right, they probably aren’t
  - Always lookup the company’s number and use that to call back
- Fully configure your VoIP systems (or find someone who can)
  - Just because it works out of the box doesn’t mean it is configured well out of the box
- Keep a limit on calling credit in case of abuse
- Not just with VoIP, all system accounts should be changed from default and user access should be reviewed at least annually. Preferably quarterly (RN)

Proactive Defense

- Have authentication policies in place. Use unique SIP credentials, have tooling to block peers after bad attempts
- Enforce access control, don't allow people to have access to calling features they don't need
- Use encryption for SIP/RTP (SIPS/SRTP)
- Educate users on best practices, vishing can be just as detrimental as email phishing!
- Yes, your employees are your fist line of defense. Arm them with the knowledge to protect your organization (RN)

THANK YOU!

- Mike Dank
- mike@philtel.org
- https://philtel.org

philtel

A PHREAKY PHONE COLLECTIVE