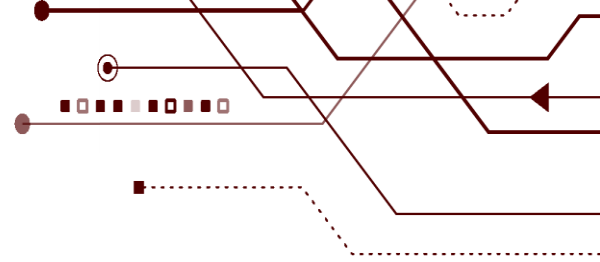


Welcome



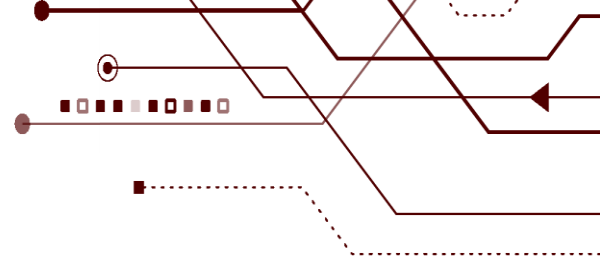
★ 2019 ★ Small Business Forum

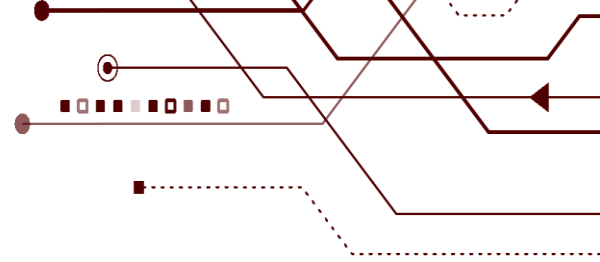
The Weakest Link in Cybersecurity ...

Breaking down the dangers of social engineering



Password Video



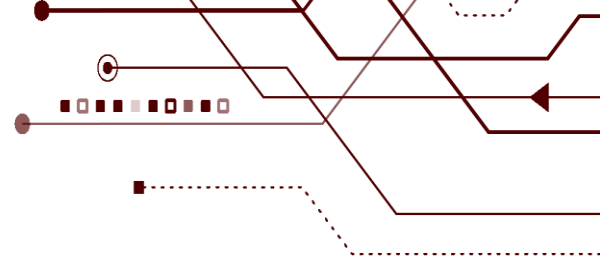


First, let's have password humor

PASSWORDS are like SOCKS...

1. Change them regularly
2. Don't leave them on your desk
3. Don't loan them to anyone
4. Don't use the same pair for all occasions





MISSION

The Texas A&M Engineering Extension Service (TEEX) makes a difference by providing training, developing practical solutions and saving lives

- Emergency Services
- Homeland Security
- Infrastructure & Safety
- Disaster Response & Recovery
- Software Development
- Cybersecurity Training and Assessments
- Manufacturing Assistance
- CNC/Welding Training Programs
- Veteran Training



John Romero

- Software developer
- Cybersecurity instructor
- Geek
- Outdoorsman



Program Director
John.romero@teex.tamu.edu



Software solutions



Cybersecurity

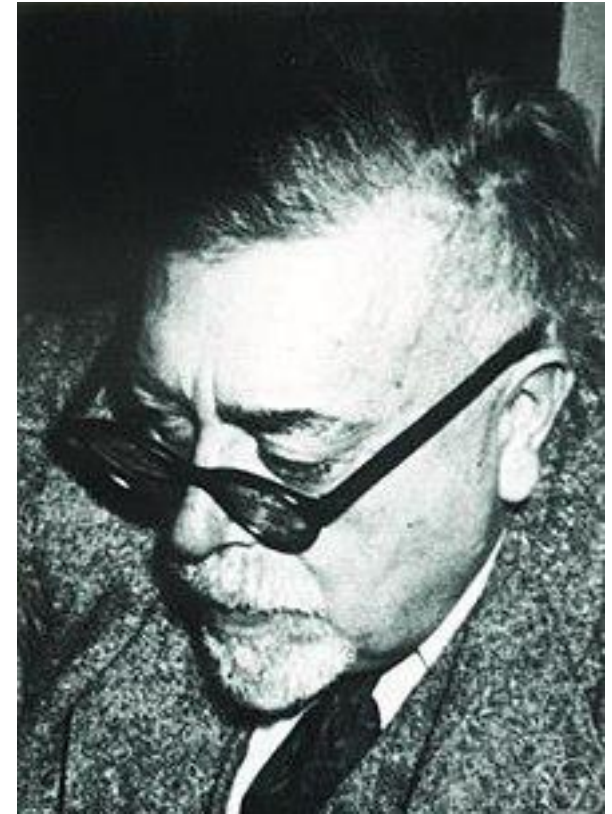
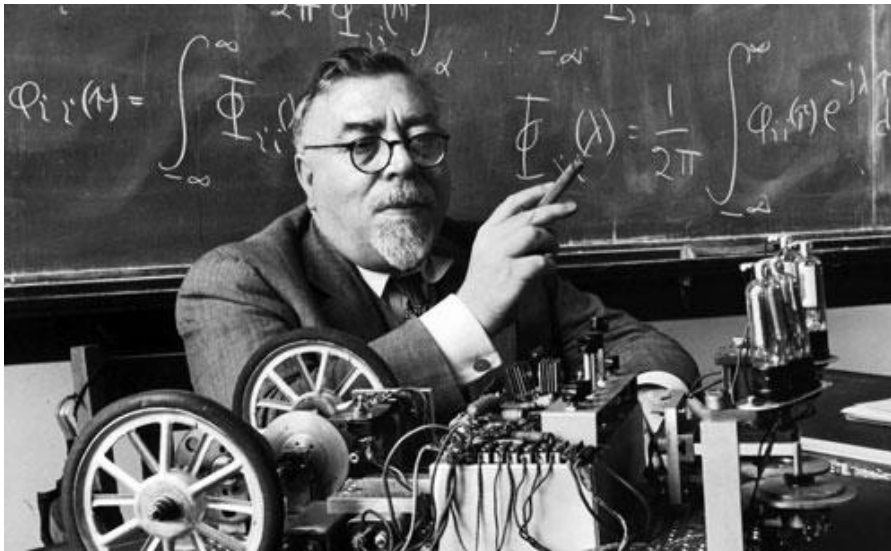


Cyber History

'Cyber' is from the Greek word for navigator.

Norbert Wiener coined 'cybernetics' around 1948

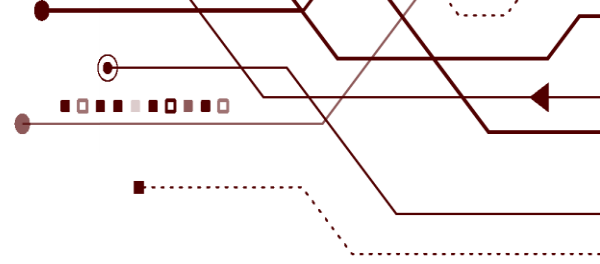
Cybernetics ...the science of communications and automatic control systems in both machines and living things...



Norbert Wiener



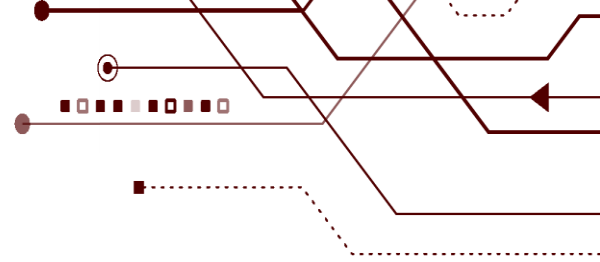
Cybersecurity - CIA



Not this CIA



Cybersecurity Definition

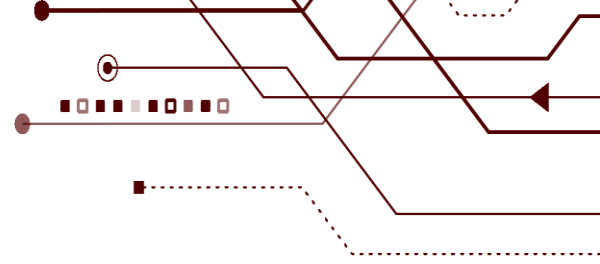


Cybersecurity – computer security, physical security, information security

- Hardware
- Software
- Policies/procedures
- Plans
- Training
- Physical security (i.e. controlled access, locked equipment, etc.)
- Personnel security (i.e. screening process, background checks, etc.)
- 3rd Party Access security - Pivoting



Social Engineering – Hacking the Mind

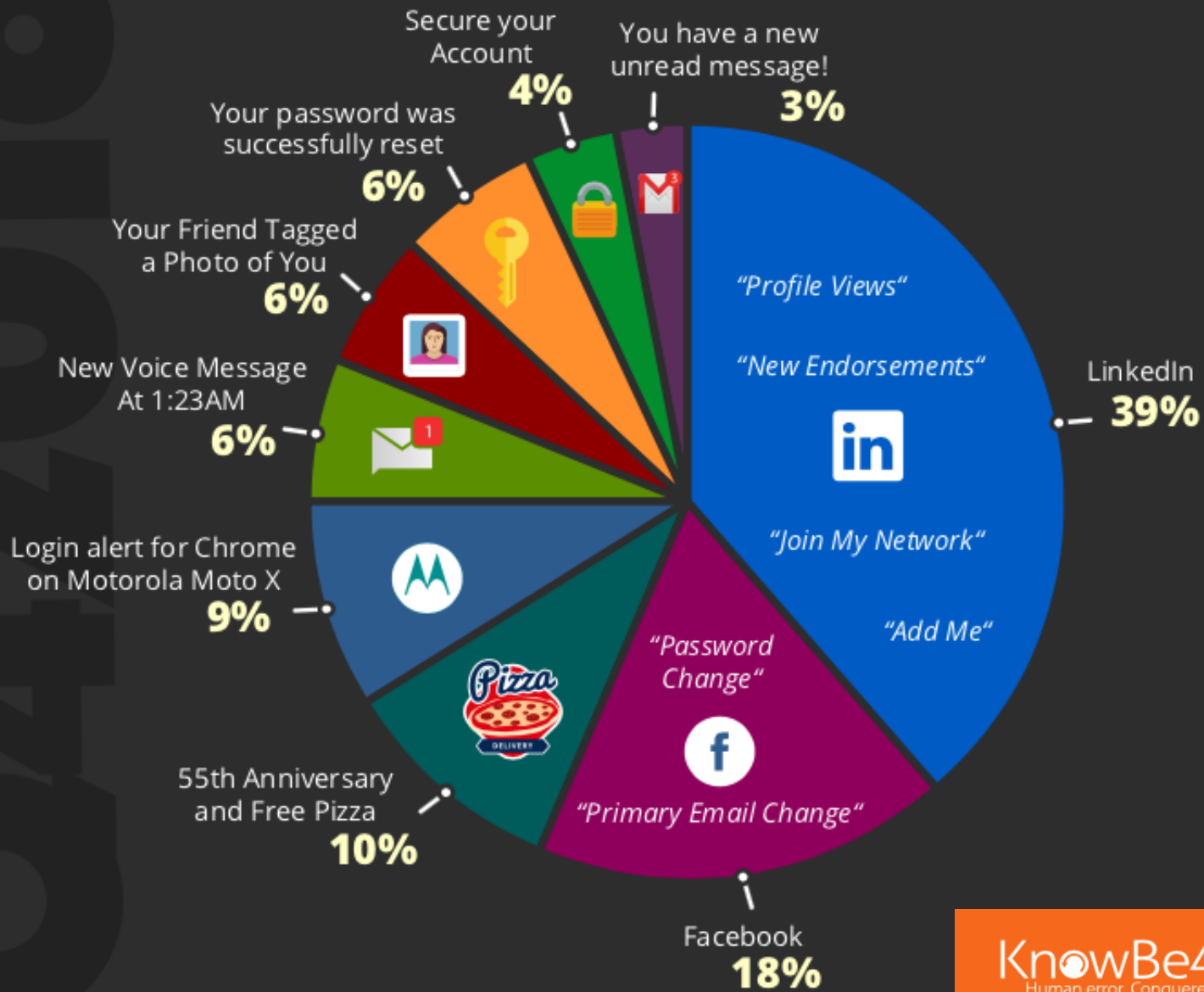


Human Vectors











- Ransomware/Blackmail
- Flash drives
- Social Engineering
 - Phishing/Smishing/Vishing
 - Dumpster Diving
 - Shoulder Surfing
 - Face-To-Face



TOP SOCIAL MEDIA EMAIL SUBJECTS



TOP 10 GENERAL EMAIL SUBJECTS

	Password Check Required Immediately	19%
	Your Order with Amazon.com/Your Amazon Order Receipt	16%
	Announcement: Change in Holiday Schedule	11%
	Happy Holidays! Have a drink on us.	10%
	Problem with the Bank Account	8%
	De-activation of [[email]] in Process	8%
	Wire Department	8%
	Revised Vacation & Sick Time Policy	7%
	Last reminder: please respond immediately	6%
	UPS Label Delivery 1ZBE312TNY00015011	6%



- Social Engineering
 - **Fake Virtual Private Network**
 - **Man in the middle**
 - **Young people at school**



Mandatory Action Required!

(3) Virus Infection Blocked. Your Passwords are at risk

We have detected that your iPhone may be infected. Virus will steal and delete your iCloud, Photos and contacts if you don't Act Now.

Tap the button below & install VPN from iTunes. Use the VPN for 7 days Buy the premium version to stop ALL Viruses. Always use the VPN when browsing on public Wi-fi

Install

Cancel

Detected By Apple.

Jacqui's Post

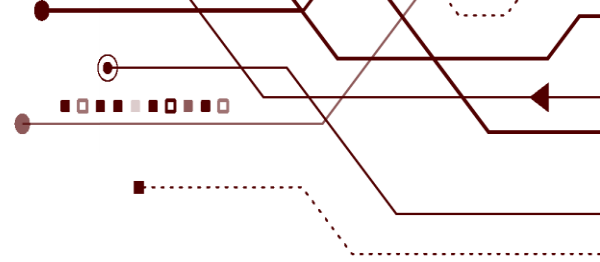
Like

Comment

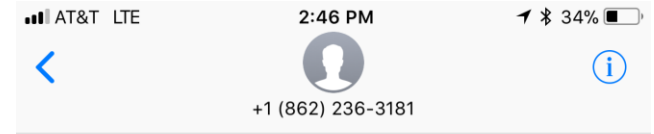
Share



Examples / Vectors of Cyber Attacks



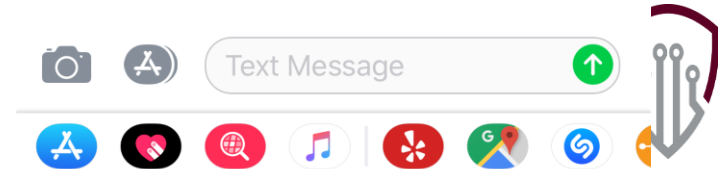
- **Smishing (SMSishing)**



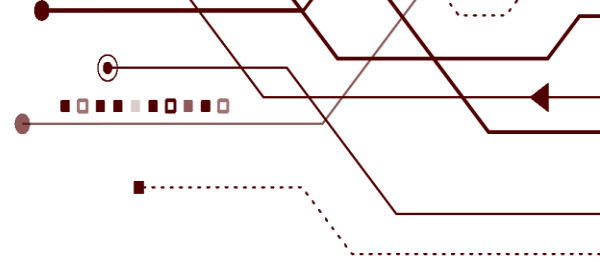
Text Message
Mon, Oct 30, 11:55 AM

You have been invited! Your friends want to hang :) Check it out! - <https://goo.gl/qWg9kX>

Reply HELP for help, STOP to stop more invites from friends



Examples / Vectors of Cyber Attacks



MS-ISAC Inbox - TEEX Yesterday at 12:53 PM M

John Romero last bill MS-ISAC
To: John Romero

MS-ISAC

Your last bill is below. Please note terms as stated on your last bill.

Account Number: D3801696

Invoice Number	Amount
8153	1,924.90

Click to connect einvoice billing

eInvoice Connect

If the above button doesn't work, please click or copy the below link to your browser

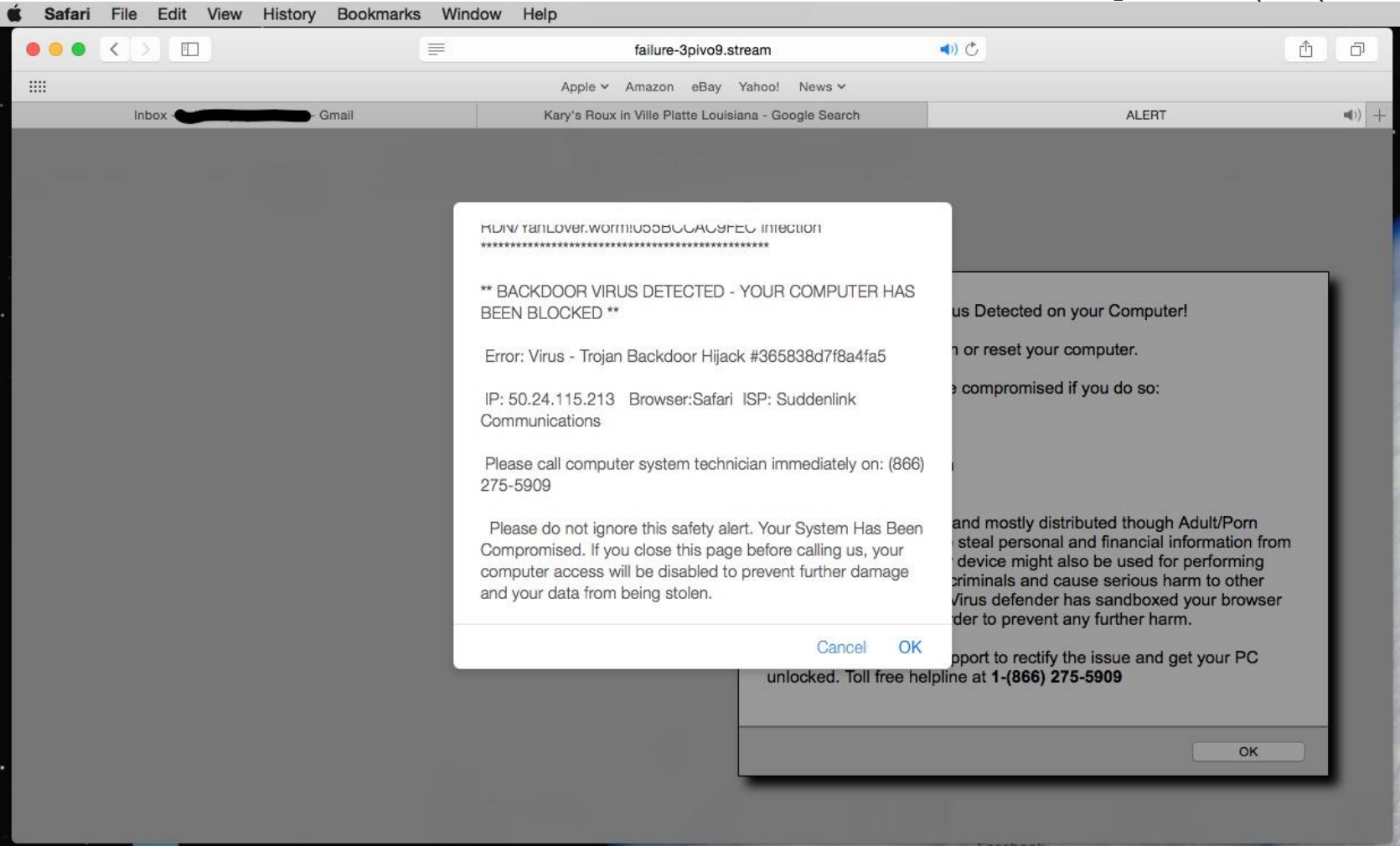
<https://sec.accs.resourses.net/>

Thank you for using MS-ISAC eInvoice Connect

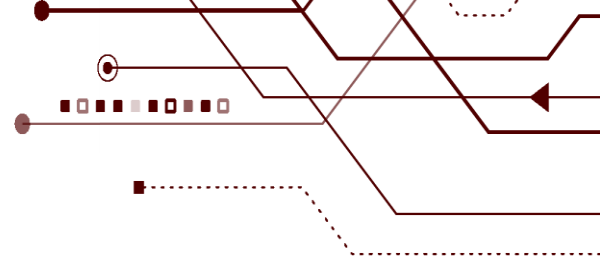
<http://awcq60100.com/sec.accounts.resourses.net/>



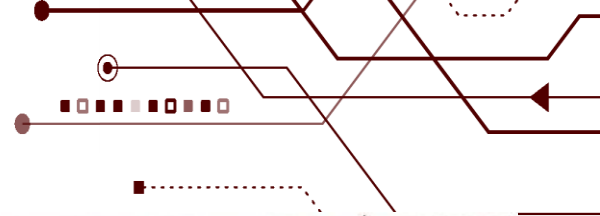
Examples / Vectors of Cyber Attacks

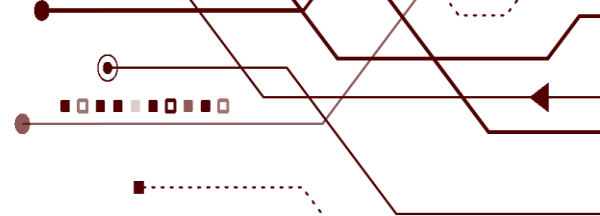


Public Wi-Fi

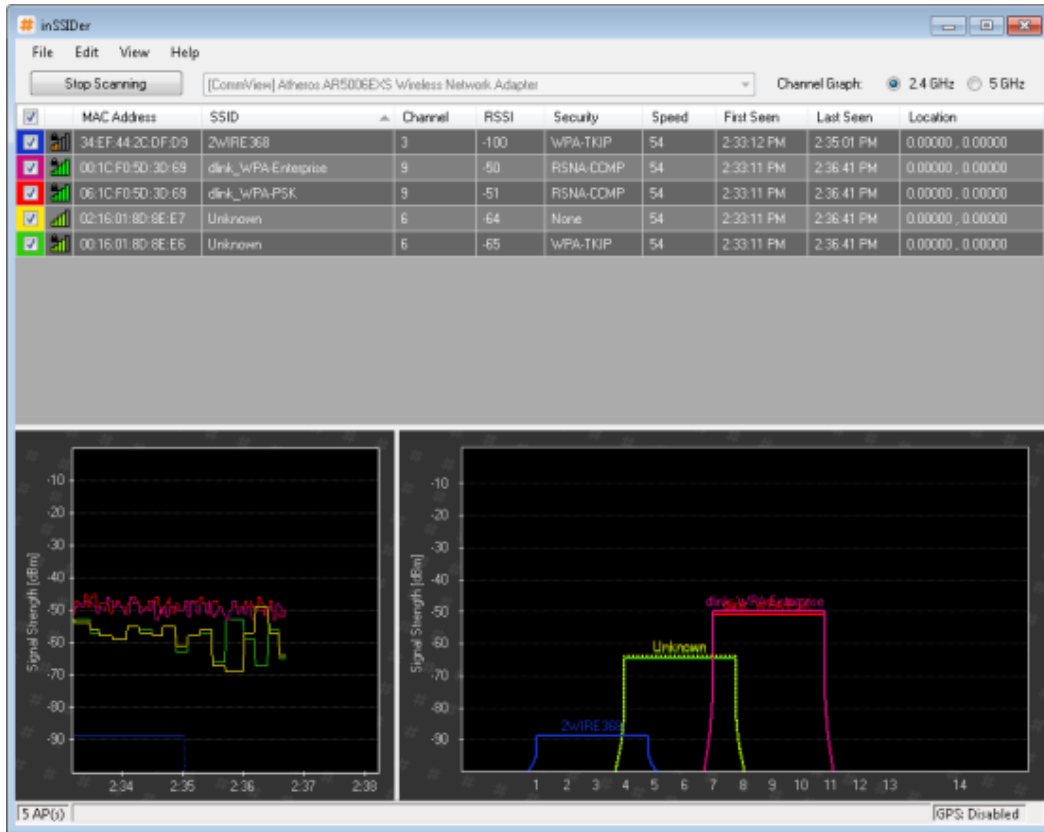
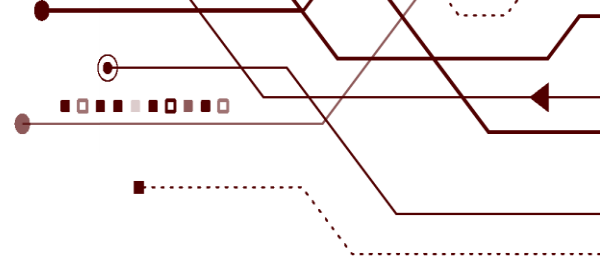


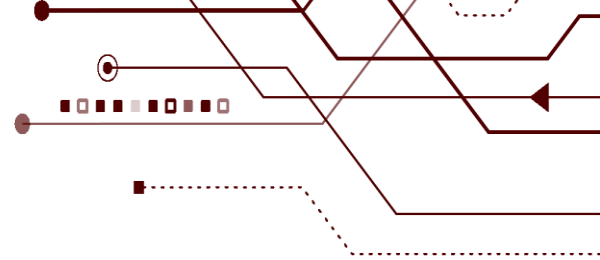
Dangers of Public WiFi





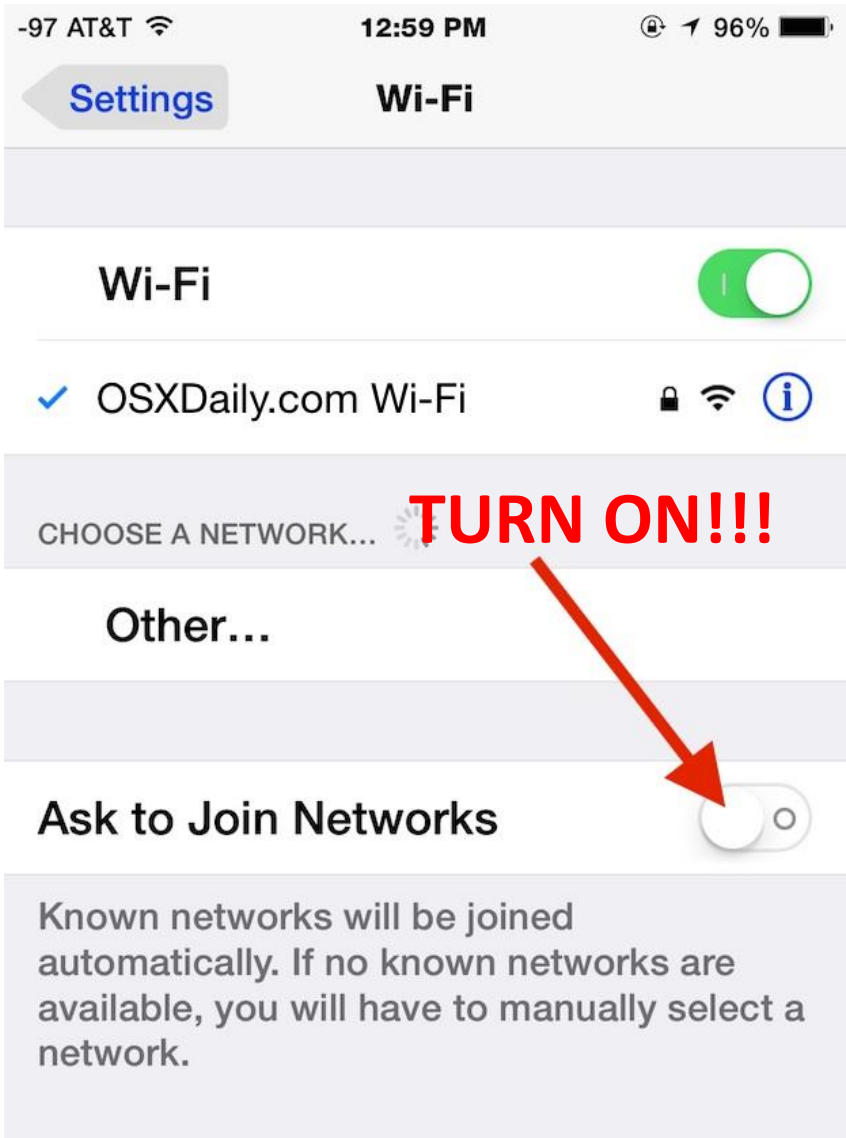
Dangers of Public WiFi



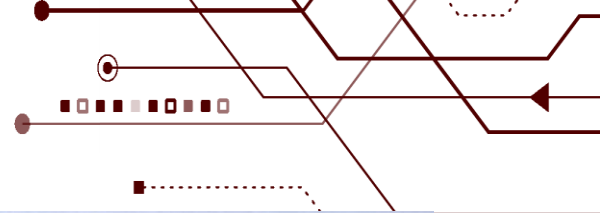


Protecting yourself – Public WiFi

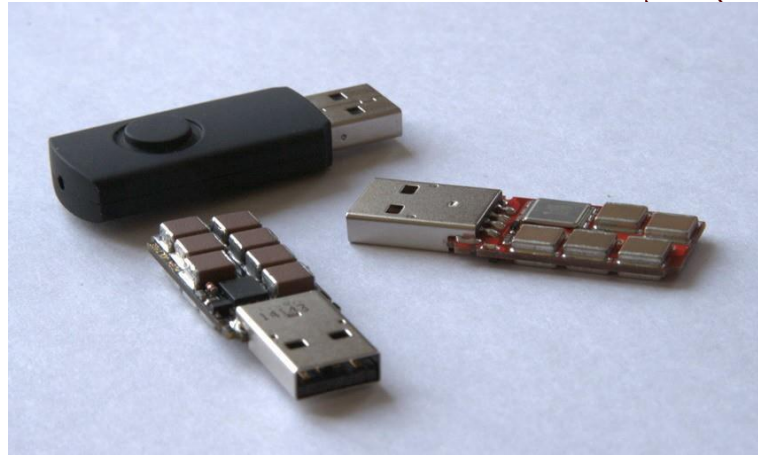
- Turn off Auto-Connect
- Keep WiFi off when not in use
- Don't connect to Unprotected
- Use a VPN



Flash Drives



*USB
Attack
Platform*



Examples / Vectors of Cyber Attacks

Bash Bunny – by Hak5



*USB
Attack
Platform*

- Flash drives





HakShop
by **HAK5**

The main logo features a stylized white outline of a robot head or a gear-like shape on the left, with a red jagged line forming a gear-like pattern above it. The text "HakShop" is written in a bold, white, italicized font with a black outline. Below it, the word "by" is written in a smaller, grey, italicized font, followed by "HAK5" in a large, bold, white font with a black outline. The number "5" is highlighted in red.

\$100.00



Introducing the Bash Bunny

The world's most advanced USB attack platform.

- Quad Core CPU
- Desktop-Class SSD
- Full Linux Distribution
- Payload Select Switch
- RGB LED Status Indicator
- Plug to Pwn in 7 Seconds



Advanced Attacks

- Driverless Multi-Gigabit Ethernet
- Fast USB 2.0 Storage
- Keystroke Injection
- Dedicated Serial Console

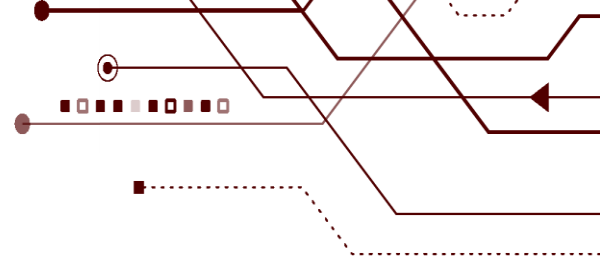
Simple Payloads

- Extendable Bunny Scripting Language
- Centralized Payload Library



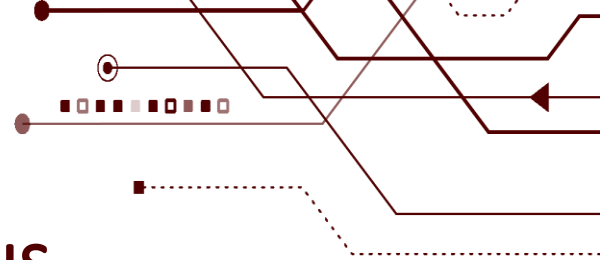
BashBunny.com





Hacking the mind is easier than hacking a computer

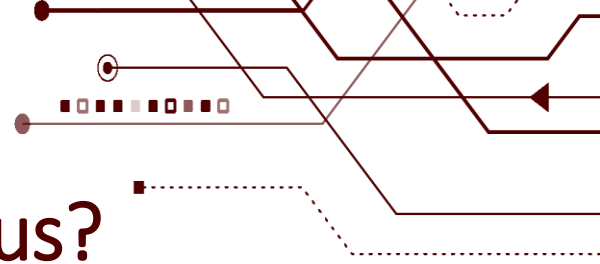




Why is Social Engineering So Dangerous

- 1. We are social creatures! We want to be helpful, therefore, you are more than capable of being easily fooled.**
- 2. Trust! There is no level of trust to avoid conflict.**
- 3. Information that you view as meaningless, we view as another price to the puzzle.**
- 4. Look nice, dress nice and talk nice are valued techniques used to dupe you on a daily basis.**





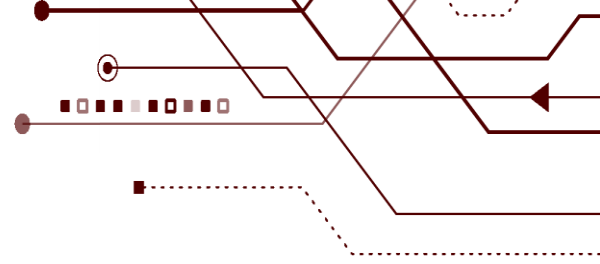
Why is Social Engineering So Dangerous?

There are several methods social engineers use to get people to do things they wouldn't ordinarily do... **PRETEXTING**

- **Persuasion**
- **Impersonation**
- **Ingratiation**
- **Conformity**
- **Friendliness**



Psychological Backdoor



We are all equipped with Psychological backdoors or triggers that are easily taken advantage of by social engineering.

Psychological Backdoor #1 – Because

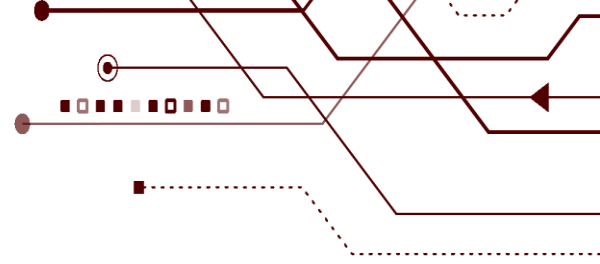
Psychological Backdoor #2 – Liking

Psychological Backdoor #3 – Confidence

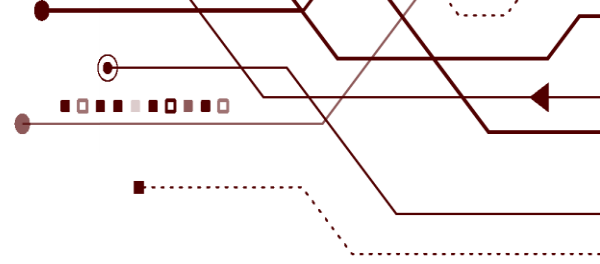
Psychological Backdoor #4 – Just Ask



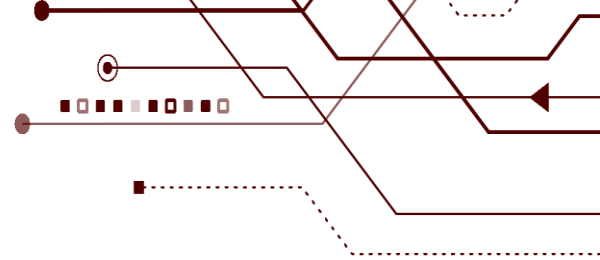
Social Media



Social Media

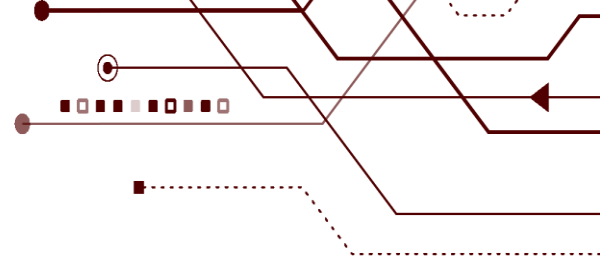


Video



Hacking the mind is easier than hacking a computer

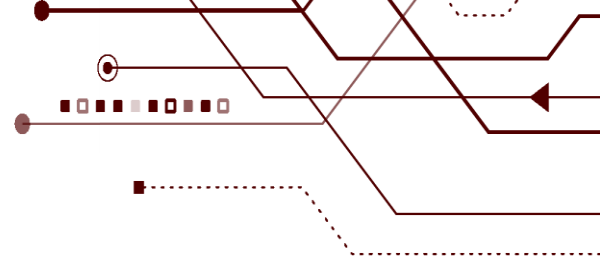




Video – Hacking a company



Hacking the company



- Spoof the number for inside the company
- Call tech support
- Have a presentation from sales - need website
- Send tech to hacked website
- Own the company ... but why are they owned?

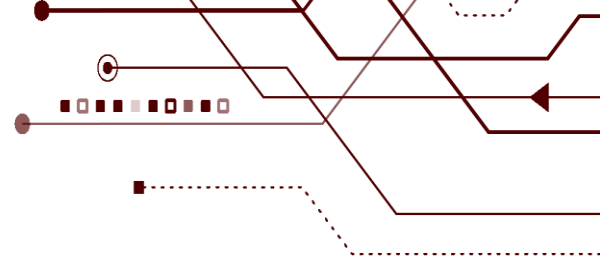




ANATOMY OF AN ATTACK



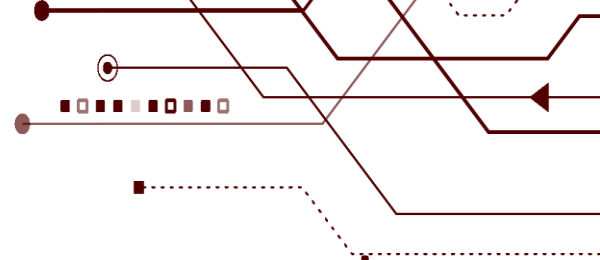
Taking down a company



- Company Earnings about to be released
- Learns about CEO (via spouse on Facebook / Social Media)
- Contacts sales via web (gets email back with company signature)
- Creates a new URL just like company (instead of dell.com = del1.com)
- Creates email to all C-Level directors – “A letter from your CEO”
- Uses signature from sales with CEO’s name and info – crafted like the ceo would use (since I’ve found out more using spouse)
- Attaches PDF (mime only) with Ransomware and exfiltration
- Releases information to web – locks up company with Ransomware

- Shorted stock of the company – how much money?





Hacking the mind is easier than hacking a computer





Video – Social Engineering

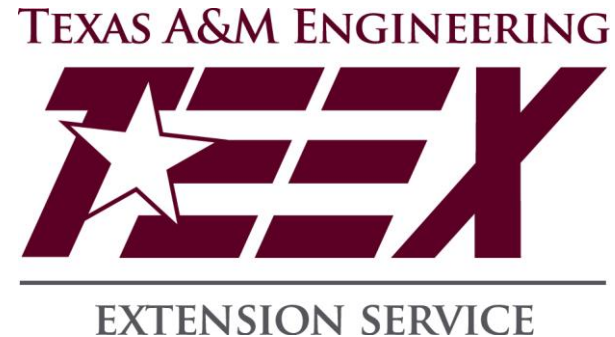


**WATCH THIS HACKER
BREAK INTO
MY CELL PHONE ACCOUNT
IN 2 MINUTES**



Thanks and remember...

- Assess
- Train
- Plan
- Exercise



John M. Romero – john.romero@teex.tamu.edu



**CYBER
READINESS
CENTER**

