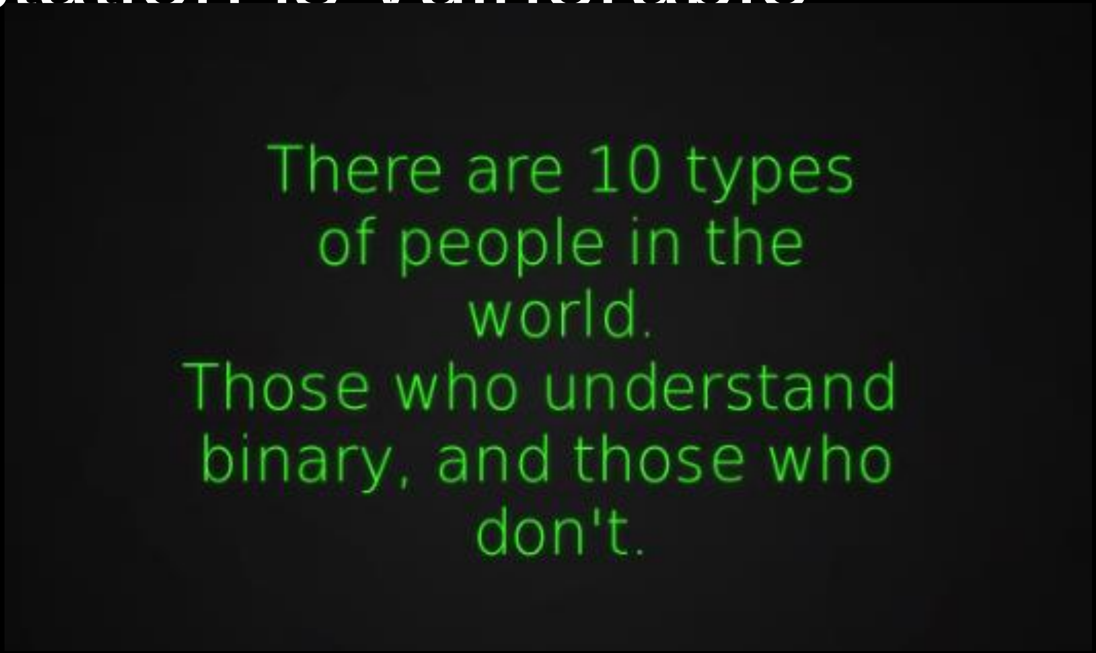
Cybersecurity for Amateur Radio

Jeri Brummett, W7WJB
Assistant Section Manager - State Government Liaison
Utah Section, ARRL
eMail: W7WJB@arrl.net
http://W7WJB.brummett.info

The Scary Cybersecurity Pitch:

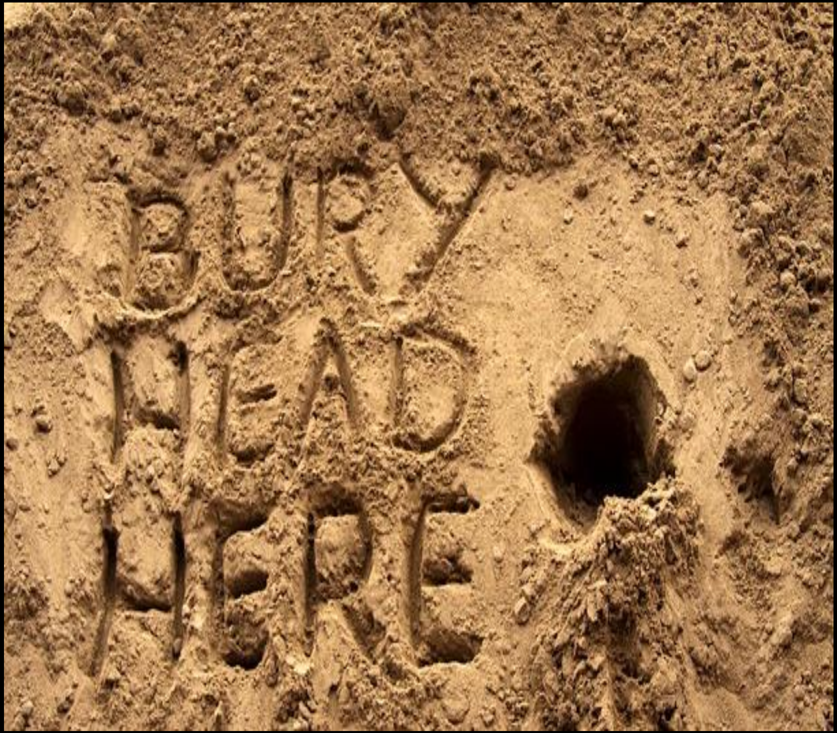
Why HAM operators should care:

- You are or will be a victim!
- Your station is vulnerable



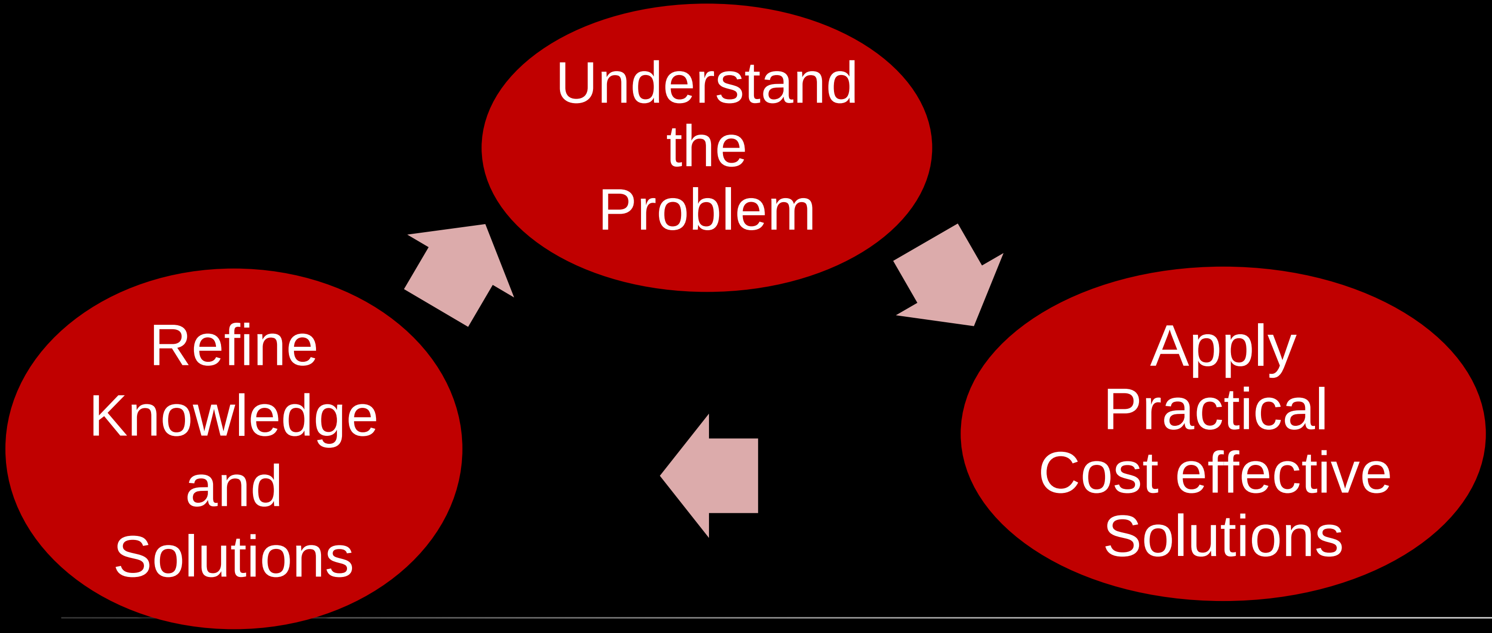
There are 10 types of people in the world.
Those who understand binary, and those who don't.

The Standard Responses:

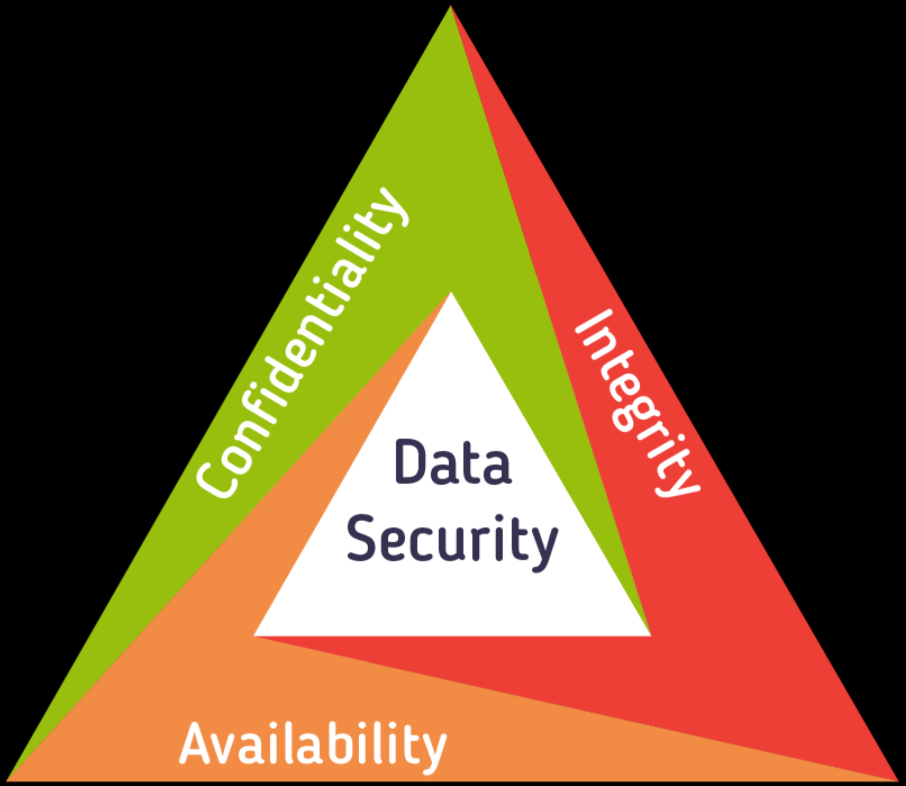


An Engineering Response:

- Engineers generally think of themselves as problem solvers who follow a systematic approach used to reach a desired solution to a problem.


Understand the Problem
Apply Practical Cost effective Solutions
Refine Knowledge and Solutions

The Security Triad:



Understand the Problem ~ Threat Actors:

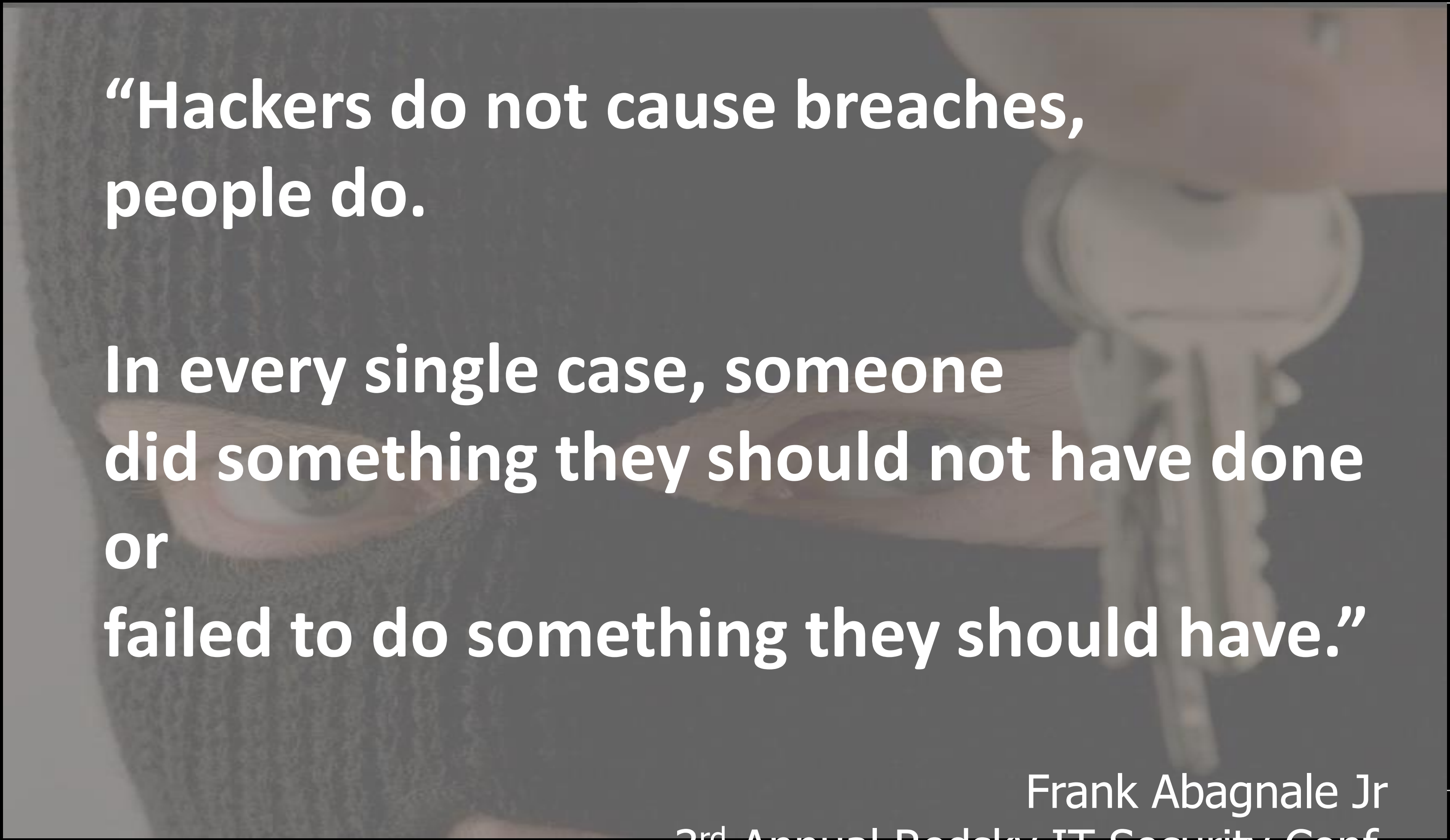
Two Groups:

- Group A
- Group B

Understand the Problem ~ Threat Vectors

- Malware
- Account Breach / Identity Theft
- Accidental Self-inflicted Threats
-
- Unsecure New Devices and “Things”
- Radio-frequency Cyberattacks

Understand the Problem ~ Our Actions:

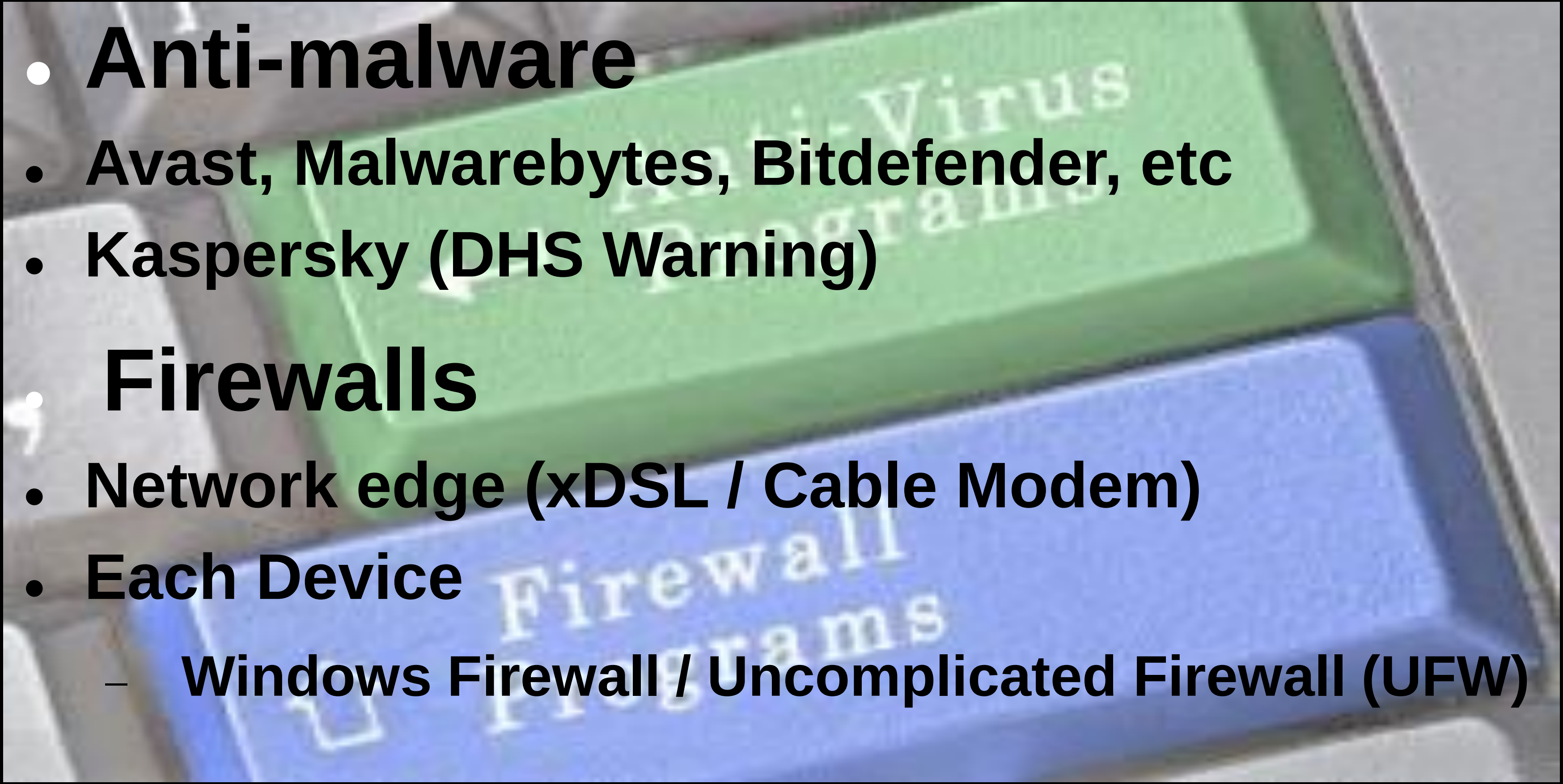


“Hackers do not cause breaches,
people do.

In every single case, someone
did something they should not have done
or
failed to do something they should have.”

Frank Abagnale Jr
3rd Annual Redsky IT Security Conf.

Problem to Practical Solutions ~ Malware



- **Anti-malware**
- **Avast, Malwarebytes, Bitdefender, etc**
- **Kaspersky (DHS Warning)**
- **Firewalls**
- **Network edge (xDSL / Cable Modem)**
- **Each Device**
  - **Windows Firewall / Uncomplicated Firewall (UFW)**

Problem to Practical Solutions ~ Account Breach / Identity Theft

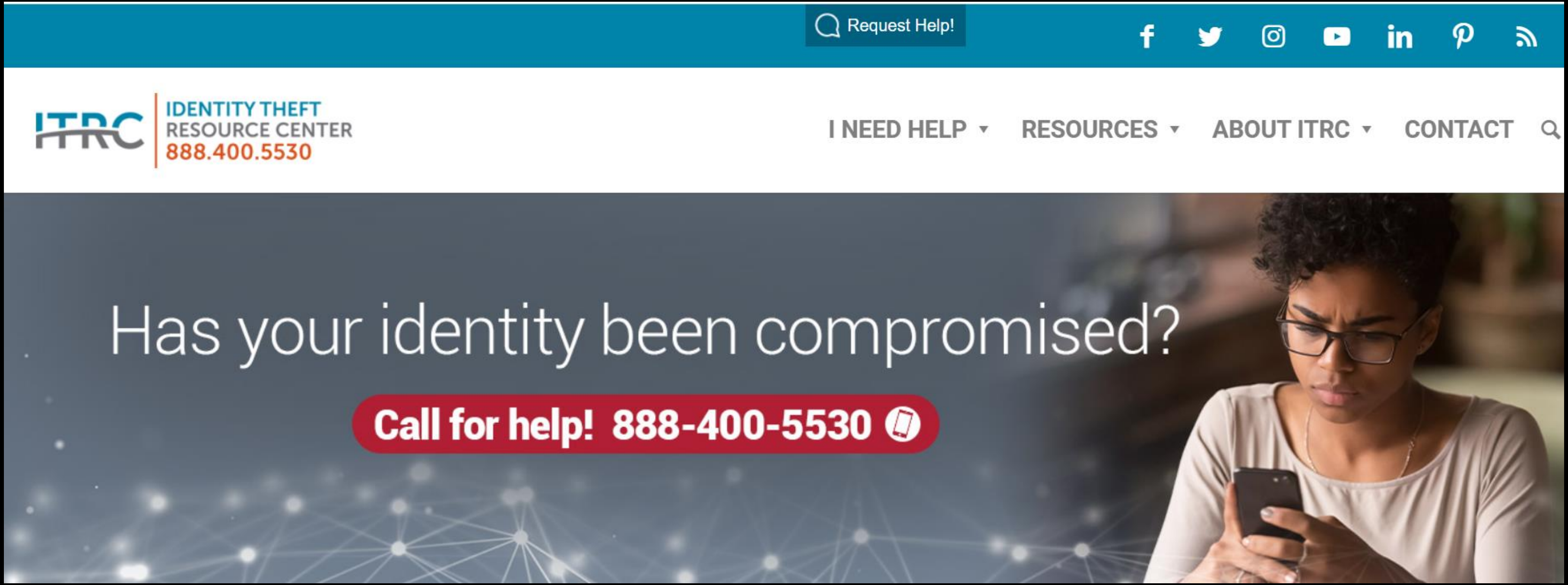
- Insider Secret: Your Identity is already compromised and for sale.
  - Info sold by same people selling you ID Theft Protection
  - $1M is not real protection...less than $2000
- Account Monitoring … Necessary Nuisance
  - Typically free

Problem to Practical Solutions ~ Account Breach / Identity Theft

- STOP … THINK … then CONNECT maybe
- Passphrases NOT Passwords
  - Password Vault
- Monitor for symptoms
  - Sudden file changes, Locked user accounts, changes in performance, abnormal system behavior, or unusual account activity.

- Problem to Practical Solutions ~

Account Breach / Identity Theft



Request Help!

ITRC IDENTITY THEFT RESOURCE CENTER 888.400.5530

I NEED HELP ▾ RESOURCES ▾ ABOUT ITRC ▾ CONTACT

Has your identity been compromised?

Call for help! 888-400-5530

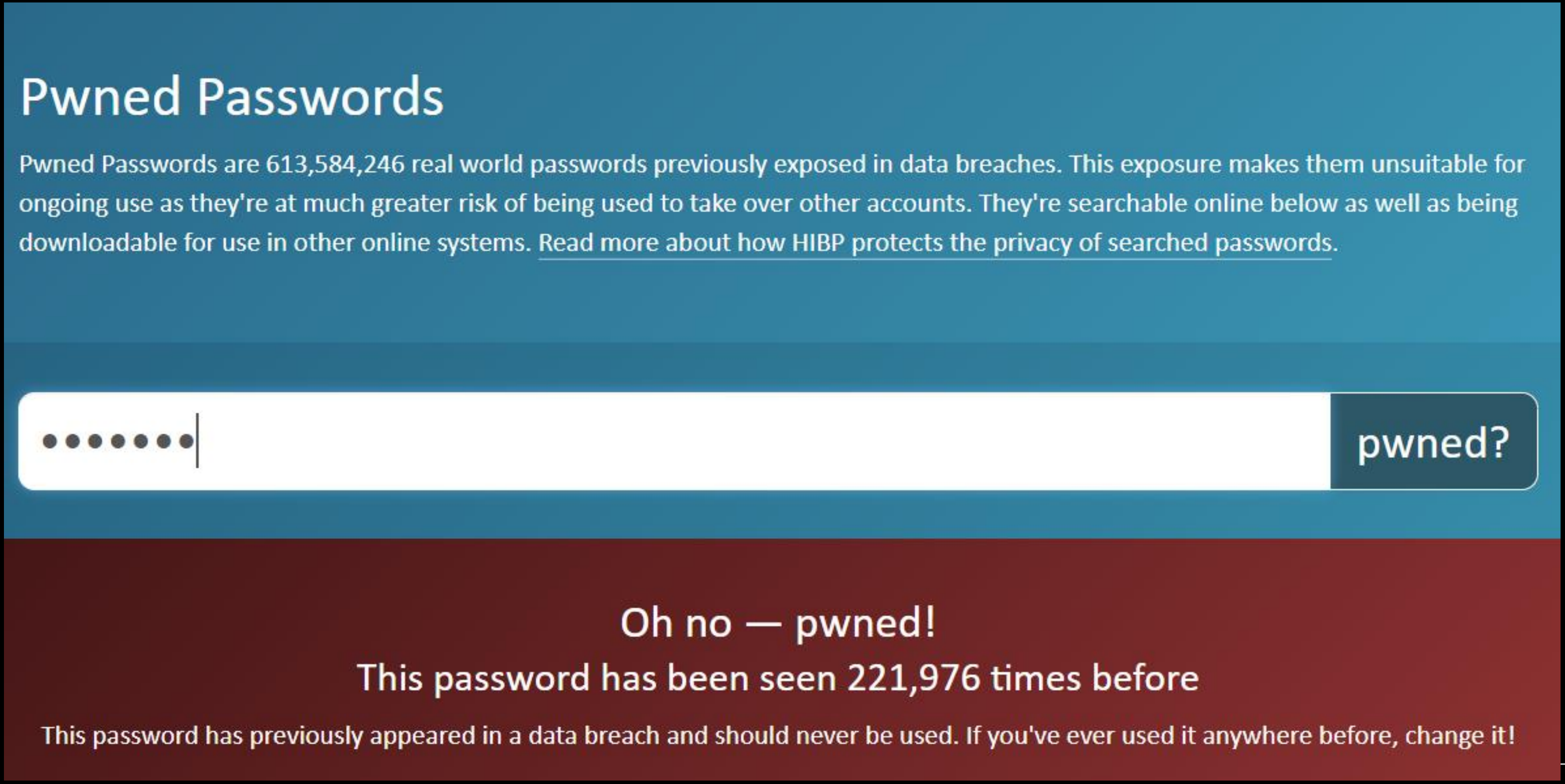
Problem to Practical Solutions ~ Passwords

- 59% use the same passwords across multiple accounts
- 50% haven’t changed their social network passwords for a year or more; 20% have never changed their social network passwords.
- 30% have used or still use birthdays, addresses, pet names or children names for their work passwords.
- 25% said they change their password at work only when the system tells them to.
  - ~Thycotic, May 27, 2017

• Problem to Practical Solutions ~ Passphrase

- Typically easier to remember and type
- Typically not in dictionaries and cracking tables
- Make up a phrase off the top of your head
  ex: Tube Steaks are Hot Dogs ← 20 chars
  Tube_steaks_R_hot_Dogs ← 22 chars
  Tube_5teak5_R_h0t_D0g5 ← 22 chars
  Tube_5teak5_R_h0t_D0g5-QRZ ←customised
- Have a “Throw Away’ passphrase
- Use a password vault

Problem to Practical Solutions ~ Pwned



Pwned Passwords

Pwned Passwords are 613,584,246 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.

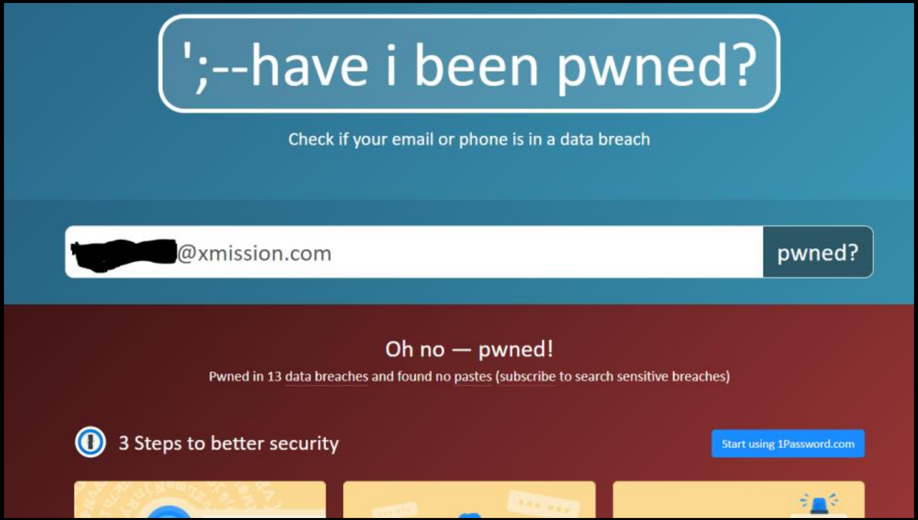
•••••••

Oh no — pwned!

This password has been seen 221,976 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

Problem to Practical Solutions ~ Pwned



';--have i been pwned?

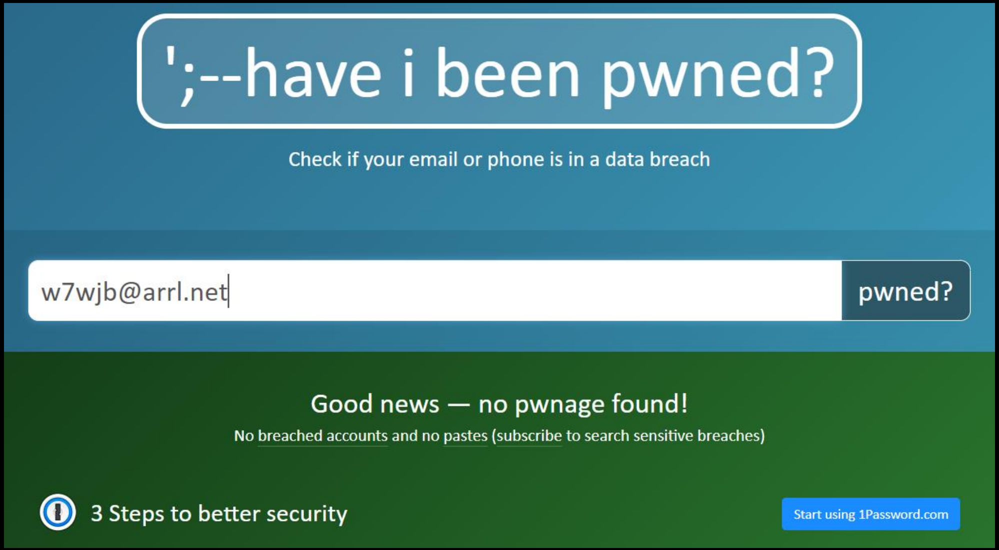
Check if your email or phone is in a data breach

[redacted]@xmission.com

Oh no — pwned!

Pwned in 13 data breaches and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security



';--have i been pwned?

Check if your email or phone is in a data breach

w7wjb@arrl.net

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

3 Steps to better security

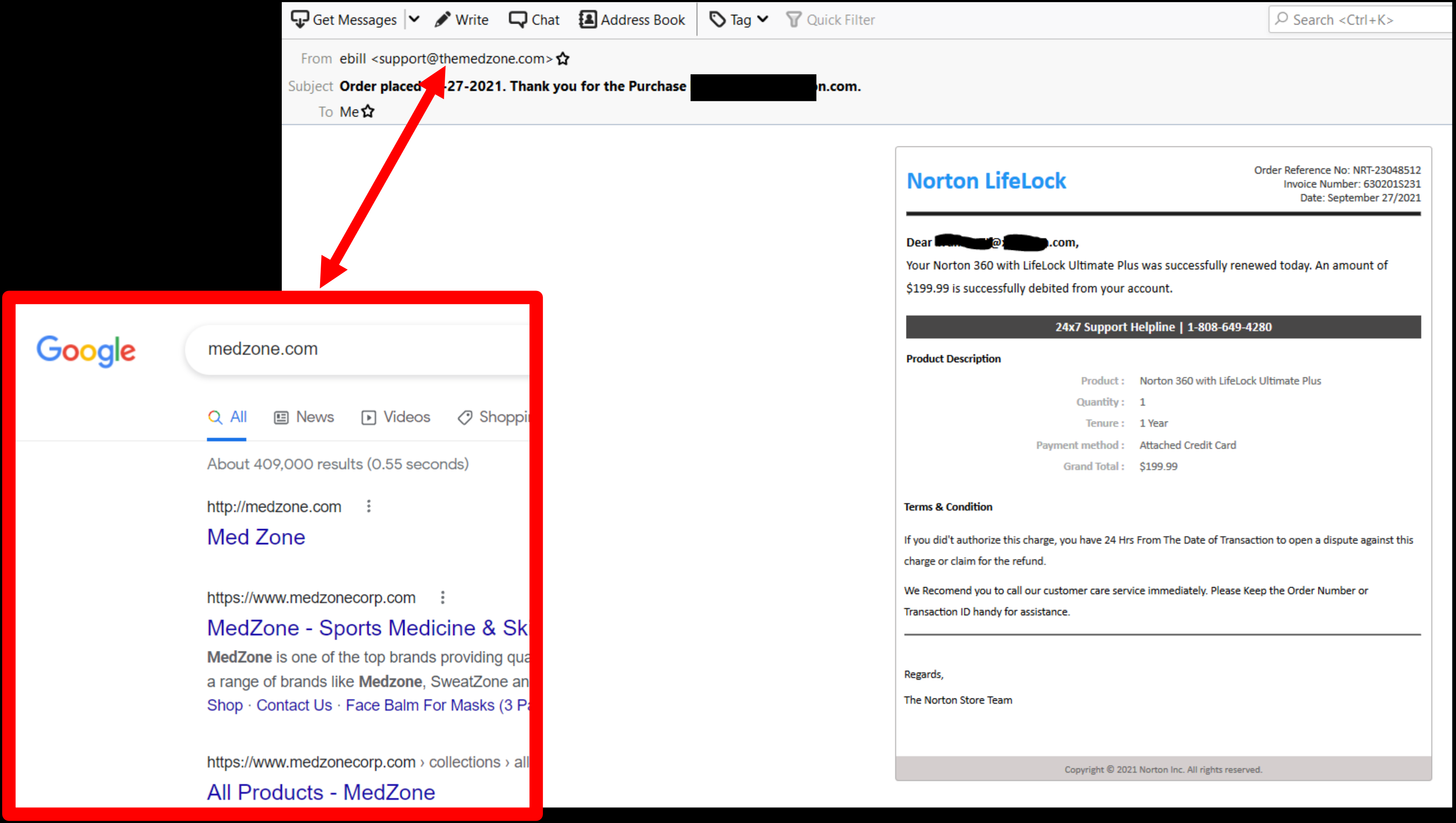
Problem to Practical Solutions ~ Accidental Self-inflicted Threats

- Change default passwords
  - Routers, modems, Raspberry Pi
- Back It Up Or You’ll Be Sorry!
- Skipping updates and scans
- Visiting bad neighborhoods and unknown places

Problem to Practical Solutions ~ Backups

- **Back It Up Or You’ll Be Sorry!**
- SSD and Cloud Options
  - Consider Encryption
-
  -

Problem to Practical Solutions ~ Phishing



From ebill <support@themedzone.com>

Subject **Order placed -27-2021. Thank you for the Purchase [redacted] n.com.**

To Me

Norton LifeLock

Order Reference No: NRT-23048512
Invoice Number: 630201S231
Date: September 27/2021

Dear [redacted]@[redacted].com,

Your Norton 360 with LifeLock Ultimate Plus was successfully renewed today. An amount of $199.99 is successfully debited from your account.

24x7 Support Helpline | 1-808-649-4280

Product Description

Product :	Norton 360 with LifeLock Ultimate Plus
Quantity :	1
Tenure :	1 Year
Payment method :	Attached Credit Card
Grand Total :	$199.99

Terms & Condition

If you did't authorize this charge, you have 24 Hrs From The Date of Transaction to open a dispute against this charge or claim for the refund.

We Recomend you to call our customer care service immediately. Please Keep the Order Number or Transaction ID handy for assistance.

Regards,

The Norton Store Team

Copyright © 2021 Norton Inc. All rights reserved.

medzone.com

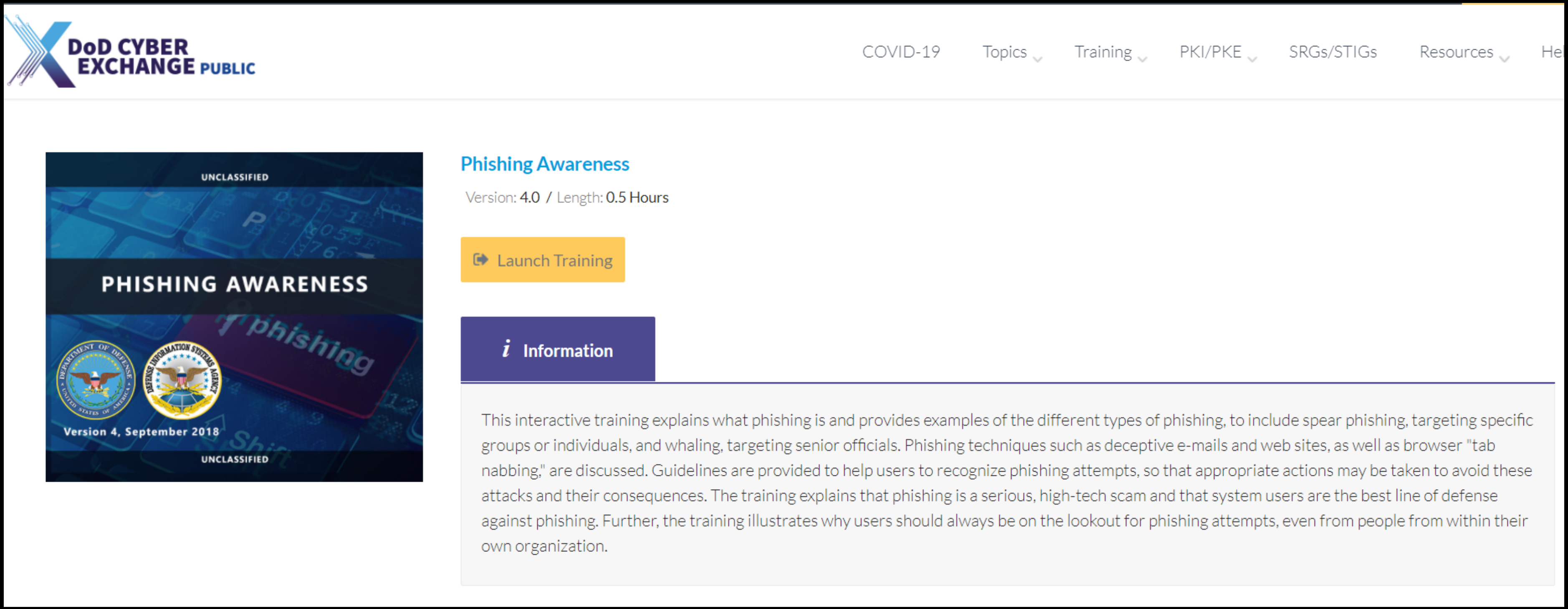
About 409,000 results (0.55 seconds)

http://medzone.com
Med Zone

https://www.medzonecorp.com
MedZone - Sports Medicine & Sk
MedZone is one of the top brands providing qua
a range of brands like **Medzone**, SweatZone an
Shop · Contact Us · Face Balm For Masks (3 P

https://www.medzonecorp.com › collections › all
All Products - MedZone

Problem to Practical Solutions ~ Phishing



Phishing Awareness

Version: 4.0 / Length: 0.5 Hours

This interactive training explains what phishing is and provides examples of the different types of phishing, to include spear phishing, targeting specific groups or individuals, and whaling, targeting senior officials. Phishing techniques such as deceptive e-mails and web sites, as well as browser "tab nabbing," are discussed. Guidelines are provided to help users to recognize phishing attempts, so that appropriate actions may be taken to avoid these attacks and their consequences. The training explains that phishing is a serious, high-tech scam and that system users are the best line of defense against phishing. Further, the training illustrates why users should always be on the lookout for phishing attempts, even from people from within their own organization.

Problem to Practical Solutions ~ Hackers

-
- Not as easy as TV and media portray
  - Hack iPhone in <30 Seconds
- China, Russia, Cancel Culture
  - Software, component, device origin matters
  - APPs, packages, firmware
- Unsecure New Devices and “Things”
  - Devices with built-in malware and breachware
  - Huawei, Hytera, etc.

Understand the Problem ~ RF Cyberattacks

- Mobile, wireless, and IoT devices all operate within the radio frequency (RF) spectrum. Due to the lack of visibility of wireless communications, devices roam freely and are often undetected and un-monitored
- Hackers can often easily compromise these devices.
- SDR systems have shown to be vulnerable
- Opportunity for HAM research

OMG: Will it ever end?

Jay Brummett, W7WJB
Assistant Section Manager -
State Government Liaison
Utah Section, ARRL
eMail: W7WJB@arrl.net
http://W7WJB.brummett.info