SOUTHERN TITLE®

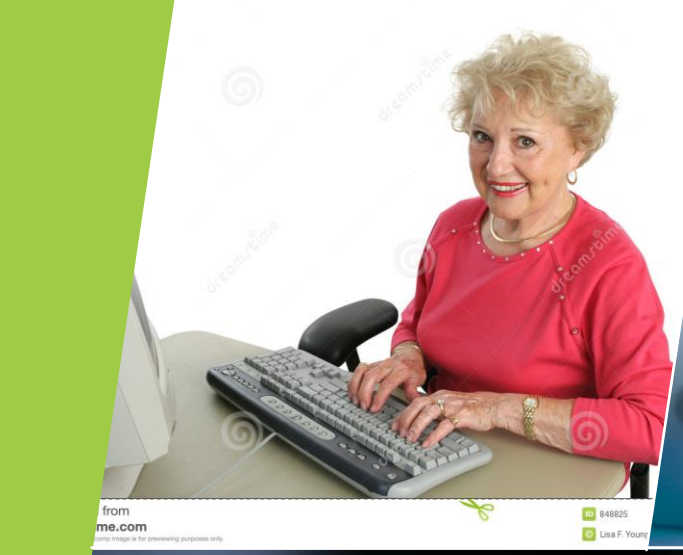
Identity Theft

Why You Are A Target!

What Crime Used To Be

- Depended on physical location
- Physically interact with their victims
- Exposed to a great deal of risk

Crime Has Changed



Now It Could Look Like This

Cyber Crime

- Can easily target most anyone in the world.
- Little or not cost.
- Very little risk.
- Cyber crime has become highly organized enabling them to be more effective

They do not know their victims.

But why me??

They attempt to hack anyone connected to the internet.

So What Is All This Jargon????

cracker -- a term sometimes used to refer to a hacker who breaks into a system with the intent of causing damage or stealing data

cybercrime -- crime related to technology, computers, and the Internet

encryption -- the process of protecting information or hiding its meaning by converting it into a code

hacking -- original term referred to learning programming languages and computer systems; now associated with the process of bypassing the security systems on a computer system or network

hijacking -- the process of taking over a live connection between two users so that the attacker can masquerade as one of the users

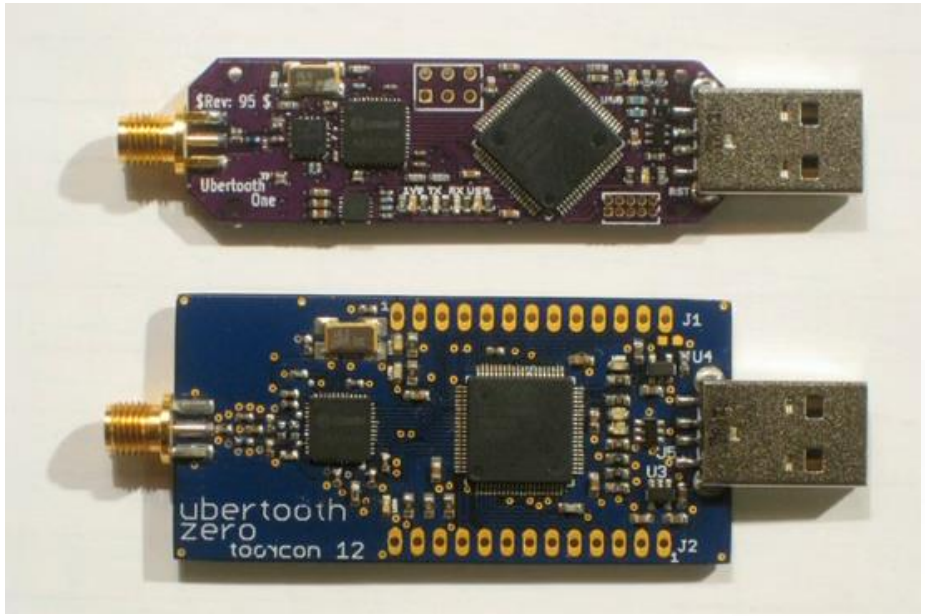
malware -- software that is intended to damage or disable computers and computer systems.

sniffer -- a program designed to capture information across a computer network

virus -- a computer program designed to make copies of itself and spread itself from one machine to another without the help of the user

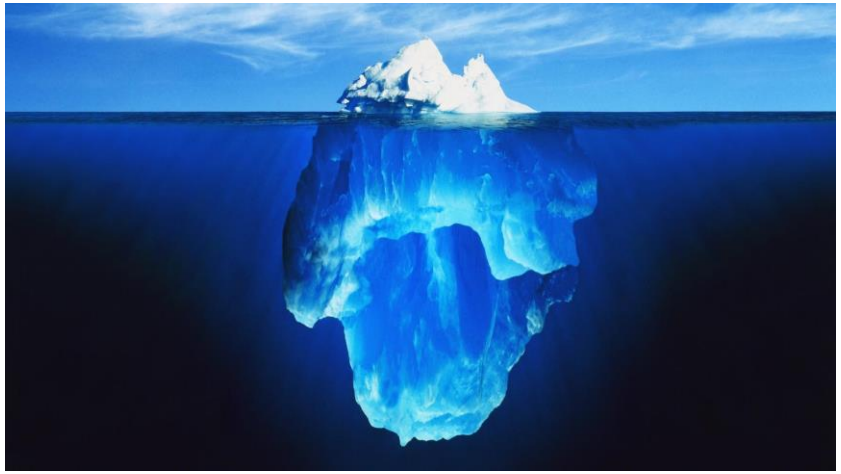
worm -- a computer program that copies itself across a network

Sniffing Devices



How do they get my information?

Stolen Credit Cards



Dark Web/Deep Web

Hacked Bank Accounts

Compromised Passwords

Phishing Emails

01

Phishing Email

02

Script

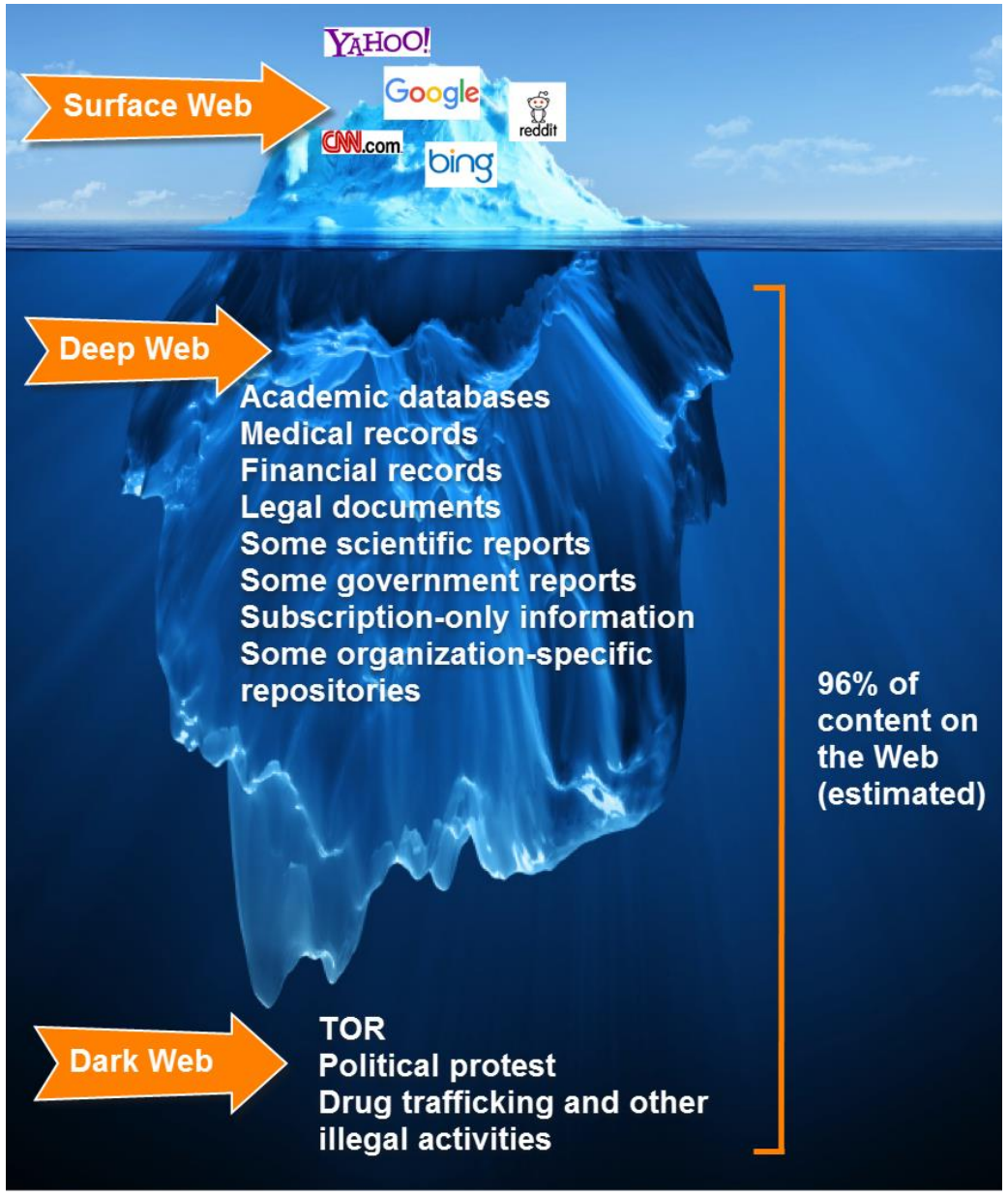
03

Malware

How The Phishing Email Works

RansomWare

- Phishing Email
- Malicious Website with link
- USB drive



Dark Web/ Deep Web

Protect Yourself–If it seems to good to be true it probably is.

Common sense is the best defense!

- Don’t be tricked into opening an infected email attachment
- Check a link before following
- Never give password over the phone

Protect Yourself

Make sure all computers and mobile devices are fully updated and have the latest patches. This keeps you protected against the most common attacks.

Use strong unique passwords for each account. Use strong password, PIN or locking mechanism on mobile devices. Use a password manager.

Creating Secure Passwords

Storing Your Passwords

Protect Yourself

Check credit card accounts and bank accounts frequently. Monthly is not enough.

The more information you post online the more likely you may put yourself at risk. Any information you post may actually identify you as a more valuable target.

Use Your Smartphone Securely

- Strong PIN, password or passphrases
- Do not respond or click on embedded links to suspicious emails
- Use SSL encryption when even possible – Https://
- Keep optional network connections (WI-FI and Bluetooth) turned off when not in use.
- Install only the applications you need. Attackers can create malicious applications that appear legitimate but are designed to infect smartphones.

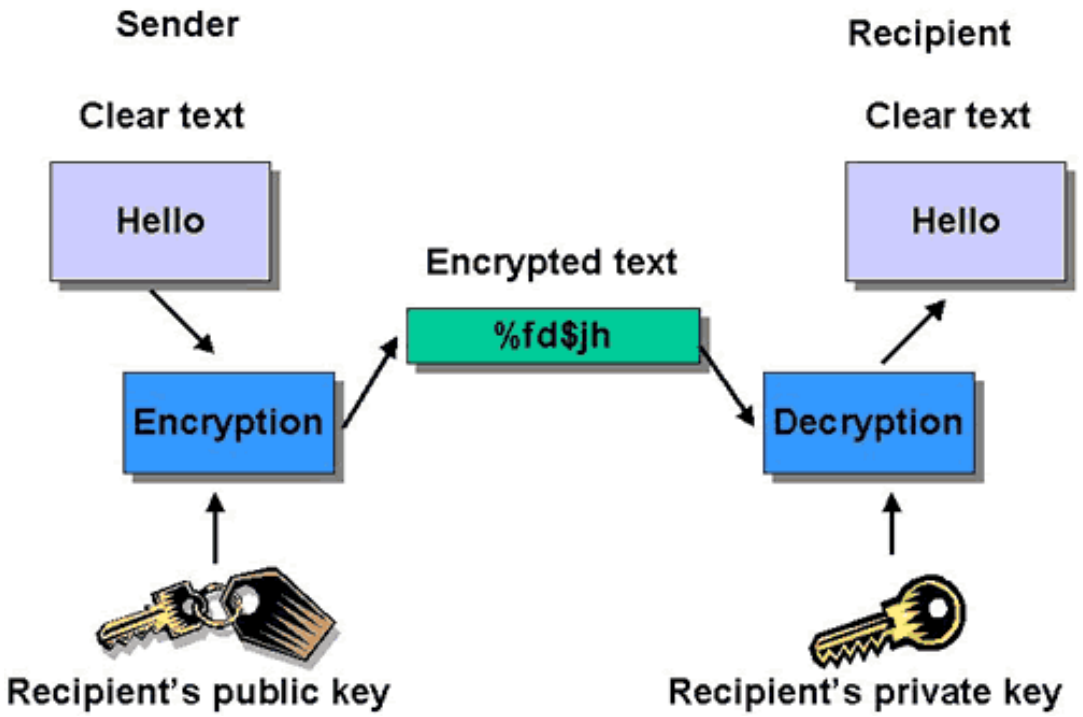
Use Your Smartphone Securely

- Keep both smartphone operating system and applications up to date.
- Be sure to back up your smartphone, in worst case scenario, you can restore its contents
- Be sure to erase all personal information securely before disposing of the phone.
- Be wary of “free” charging stations
- Set up “Find my iPhone” or “Andriod Device Manager”
- Encrypt Phone

REALTORS® Are A Target For Imposter Emails.

Protecting Your Customer

Encrypted Email



Protecting Your Customer

- During transaction make sure you are communicating regularly with all parties including lender and closer.
- Do not take wiring instructions into your possession.
- Make sure you are keeping all of their PPI in a secure location.

Protecting Your Customer

Cyber Crime Insurance

Southern Title – Protecting You and Your Customer

SOUTHERN TITLE®

Thank you and stay safe!