unifiedtrust

Traveling Security Training

Jennifer Redden
IT Director
Unified Trust Company

Agenda

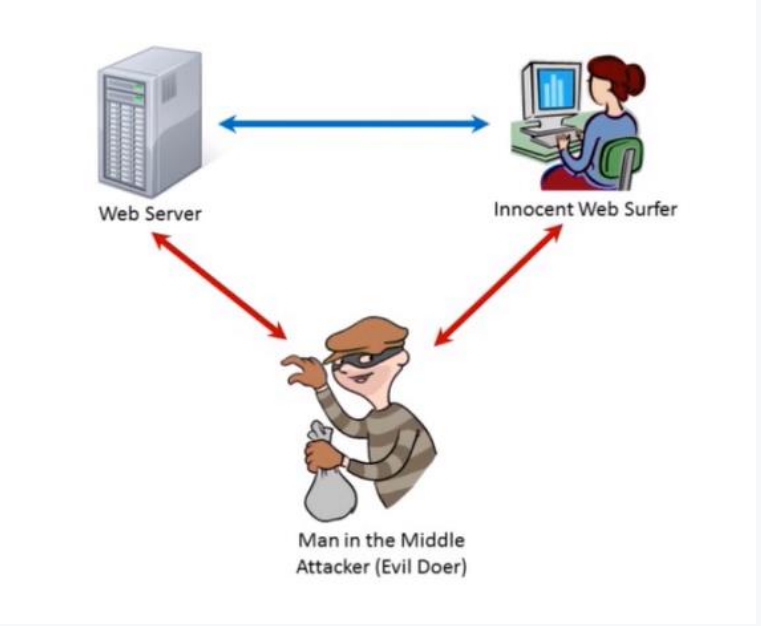
1. WiFi Attacks
2. WiFi Protection
3. Phone Attacks
4. Data Concerns

National Stats that scare us

- 1,946,181,599 – total number of records containing personal and other sensitive data that have been compromised between 1/1/2017 and 3/20/2018
- 7 in 10 of all organizations in the US were affected by a data breach
- 100% percent of organizations from a sample of 850 organizations with at least 500 mobile devices that experienced a mobile attack in 2017. In fact, organizations were attacked on average 54 times.
- In 2017, 14.5 billion malware-laced emails were sent
- In 2017, there was a 1,000% increase in phishing efforts
- In March 2018, ransomware attacks disabled critical government systems in Atlanta & Baltimore.

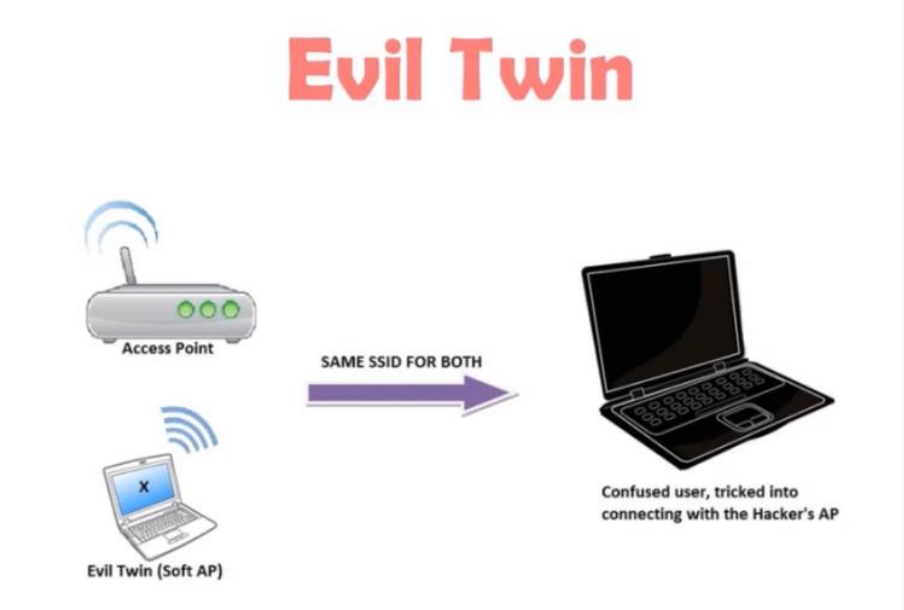
Free Open WiFi – Attack Scenario 1

- Man in the Middle Attack – Attacker secretly relays and possibly alters the communication between 2 parties who believe they are directly communicating with each other. Essentially, hijacks your internet session.
  - Example location: Restaurant/Café like Starbucks
  - Example hack: Log into bank account to move funds. Hacker intercepts information and changes account number. Wire funds to hacker's account, without realizing theft!



Free Open WiFi – Attack Scenario 2

- Evil Twin – Hackers create rogue wifi connections that appear legitimate. Unknowing users connect to the wifi network and use it for internet activity, but completely unaware that information is being collected.
  - Example location – Airports
  - Example hack – There are two free wifi's listed at the airport. You dismiss and connect to the strongest signal. This is a hacker and they can now steal all of your internet activity including user credentials, user financial information, etc.



Free Open WiFi – Attack Scenario 3

- Wireless Phishing – Hackers trick wifi users to divulge sensitive information
  - Example location – Airports or Hotels
  - Example hack – Hackers create a fake version of a web portal. This web portal requests credit card details in order to charge a small fee for internet access. The hackers enjoy a shopping spree.

WiFi Protection

Public WiFi Safety – Tips to Remember:

01

Only connect to wifi you trust

If in doubt, do not use. Hotspot from your phone is the easiest solution.

02

Encryption is your friend

Always use encryption such as https or VPN to view or send confidential material on wireless networks. Won't stop more sophisticated hackers!

03

Turn off automatic wifi connectivity on your phone

Don't leave wifi on if you aren't using it. Turn off automatic wifi connectivity so it won't actively seek out and connect to open wifi spots.

Phone Attacks

Juice Jacking

Your phone needs a recharge yet again! You don't have a charger, so you decide to you the public charging kiosk or the hotel's USB charging outlet.

Problem: the same cable used to recharge your battery in your phone, also transfers data.

Resolution:

- Do NOT use your USB to charge from unknown sources
- Take a personal charger

Smishing

Smishing is the practice of sending phishing attempts to your cell phone.

Do not click on links in texts if text message appears suspicious!

Trustjacking

*Issue found in April 2018, affects only iPhone

Previously plugging your phone into an unknown device exposed you to potential hackers. However, once the phone disconnects, hackers lost their way to pull off direct attacks. Not anymore…

Currently, a weakness in iTunes Wifi sync, allows users to sync up content and data by agreeing to "trust" the device. Hackers can remotely view victims' mobile screens, take content, and install hacker apps disguised as genuine apps.

Phone Attacks

Apps

Download with caution as that cool game can contain malware. Don't root your phone. Consider security software for your phone.

- Anti-malware: Malwarebytes
- Anti-virus: Norton or Sophos

Spear Phishing

Common Business Phishing: LinkedIn

You think it's a new potential customer who wants to connect via LinkedIn. NOPE!

They provide you a link to read, you click on it, and hackers are in!

Confidential Data Concerns - Car

How to make your data safe

Rental Car

You need to recharge your phone. If you use the USB in the car, you could get more than a charge.

Recommendations: Use a cigarette lighter charger

Rental Car

You pair your phone to talk while driving on a business trip. It downloads your information (contacts, etc.) to the rental car. You turn in the rental car and now data can be exploited.

Recommendation: Purchase a Bluetooth headset

Personal Car

Before you sell your car, be sure to clear your personal information.

Recommendations:

- Clear your address book
- Disconnect from the cloud
- Reset your garage door opener
- Clear navigation -“home”

Confidential Data Concerns - Plane

How to make your data safe

PNR Barcode = Passenger name record (Record Locator)

When you scan the barcode with your phone, you can go to their website and get typically:

- Full name
- Date of birth
- Email address
- Telephone number
- Last 4 digits of payment card used
- Passport number and details
- Details of care or hotel bookings made thru airline
- Special Service Requests (meal, upgrade, etc.)

Reduce your risk:

- Don’t post pictures of your boarding pass or luggage tags on social media
- Destroy your boarding pass and luggage tags securely