Ten Things You Can Do to Stay Safe in a Digital World

Jake Ruddy

PCS

Otherwise it wouldnt be security

IS IT SAFE?

Public WIFI

PCS

Public Wireless

NO SUCH THING AS FREE

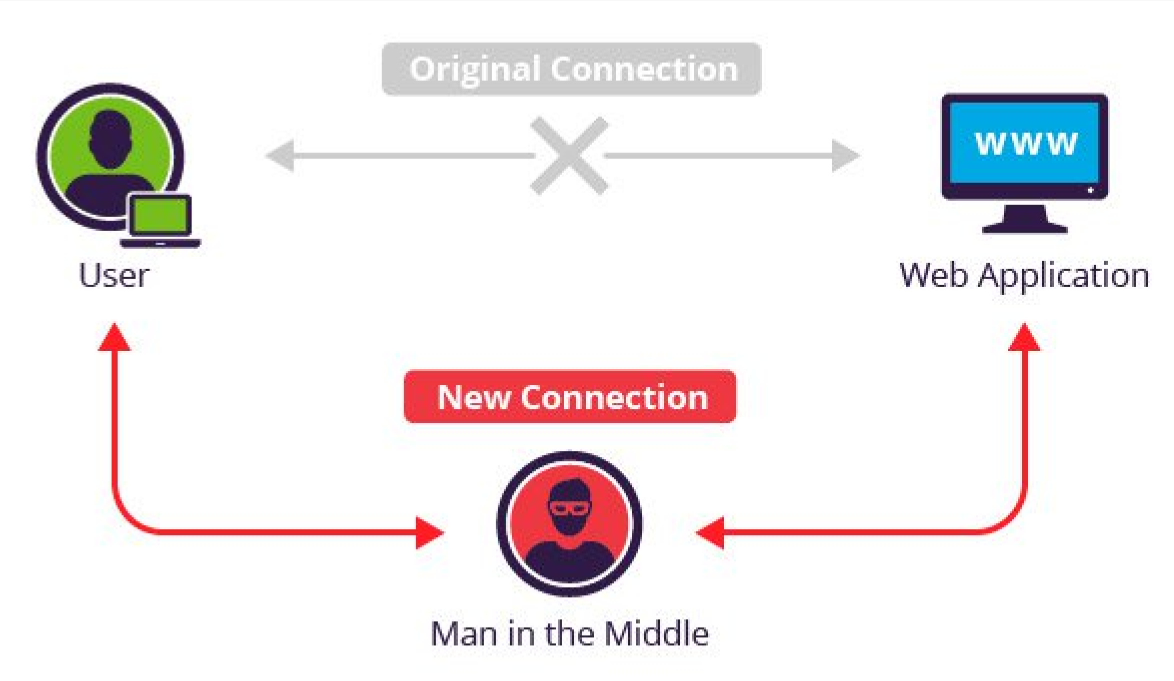
Public WIFI is not safe

- You do not know who manages the network and if it was setup in a secure fashion.
- You do not know when security updates were last applied.
- You do not know who is on that network.

Public Wireless

NO SUCH THING AS FREE

Man in the Middle Attack



Public Wireless

NO SUCH THING AS FREE

If you must:

- Personal surfing only! YouTube, NetFlix, etc.
  - No banking, credit cards, or healthcare related surfing.
  - Consider using a VPN Service (NordVPN)
- Do not do any business related work on public wireless.
  - Always use VPN
- Hotel Wireless is not guaranteed to be safe.
- Turn on “Ask to join networks”

Personal Hotspots

YOU HAVE ONE IN YOUR POCKET

Most phones today require a data plan.

- Data is getting cheaper!
- Protecting your data is worth the price.
- Shop your plans.
- If it’s your personal hotspot, you control the password and how secure it is.

ENCRYPT YOUR DATA

VPN

VPN

WHAT EXACTLY IS IT?

Virtual Private Network

VPN allows you to securely connect to a remote network using encryption.

A VPN connection can be software or hardware based.

1

You want all of your data encrypted.

- On a public wireless or just trying to be secure in general.

2

You need to access files on a remote network securely.

3

VPN is often used to connect multiple offices.

IS EMAIL SECURE?

Email Encryption

If it contains sensitive info, encrypt it

EMAIL IS SENT IN PLAIN TEXT

Email is not secure unless it’s encrypted.

- Email was not designed to be secure. It was designed to be a fast method of communication.
- 269.6 BILLION emails sent each day.
- Estimated to be over 320 BILLION by 2021.

- No business should be sending emails that contain sensitive PII (Personally identifiable information) that is not encrypted.

- There are many services available today to help encrypt email.
- Sharefile, Barracuda, Office365, most spam filters.

FREE DOESN'T CUT IT

Antivirus/Antimalware Protection

PCS

Viruses

COMPUTER CAUGHT A COLD

A computer virus is designed to spread from host to host and can replicate itself.

They often attach themselves to a legitimate program or file. Once executed it will follow a specific set of instructions.

Viruses require a user to trigger the program or boot from an infected disk or USB device.

1

Self-replicating programs were first established in 1949.

2

Frederick Cohen coined the term "Virus" for computer programs that were infectious due to their tendency to replicate in 1983.

3

Symantec launched one of the first antivirus programs called Norton Antivirus in 1990.

Ransomware

SHOW ME THE MONEY

Ransomware is malware that blocks system access until a sum of money is paid.

This form of malware has generated tens of millions of dollars to date.

It uses encryption to hold files ransom. Files cannot be restored without the keys for decryption or doing a full restore from backup.

1

Antivirus will not prevent a ransomware infection.

2

Ransomware is often deployed remotely, using an infected system. It can also be triggered by clicking a link in an email or attachment.

3

Ransomware can also be deployed via a Trojan.

Proper Protection Required

FREE WORKS, PAID IS BETTER

Antivirus and Antimalware programs provide different protection.

- These programs compliment each other.
- Antivirus is typically targeting older style viruses like trojans and worms, while antimalware is handling newer generation zero day attacks.
- Next Gen Antivirus is here and improving, usually expensive.

WHAT IS THE WEAK LINK?

Passwords

Security Starts With You

WEAK PASSWORDS ARE ASKING FOR TROUBLE

A password policy is a must

Humans are the weak link when it comes to security.

Humans can and will bypass security, sometimes unknowingly.

1

Forget “strong” passwords that are difficult to remember. Use four random words like: yellowbirdbluesquirrel

2

Never share passwords:

- Company passwords should stay internal
- Social Media passwords should be different than banking.
- Password reset questions should not be guessable

3

Password managers are helpful tools:

- LastPass
- KeyPass
- Keeper
- Dashlane

EMAIL, THE EASIEST WAY IN

Phishing Emails

Phish·ing

/’fiSHiNG/

Number one cause of data breaches

- Phishing is an attempt to gain access to sensitive information such as usernames, passwords, and credit card details.
- Email spoofing is the most common delivery method. Emails purporting to be from your bank, PayPal, cloud services, social media websites, or IT administrators encourage you to click links that redirect you to a compromised site.
- 96% of cyber attacks start via a phishing email. (Verizon DBIR 2018)

Phishing is everywhere

IT’S UP TO YOU

Phishing most often plays on fear. Other potential examples include:

- FedEx, UPS, USPS, Amazon failed delivery notices
- Coupons / Sales
- Voicemails
- Fax notices
- Fake invoices
- Overdue notices
- Fake account compromised notices
- Fake encrypted email notices
- Social media themed

Question Every Email

TAKE A DEEP BREATH

We are all busy and trying to work quickly.

It is important that you also work efficiently.

1

Read the email multiple times.

Look for:

- Spelling mistakes
- Grammar mistakes
- Calls to action
- Threatening language

2

Learn the power of the mouse hovering over a link

Does the link even make sense?

3

Hit reply to, does the email go to the correct person?

Question Every Attachment

TAKE A DEEP BREATH

We are all busy and trying to work quickly.

Slow down and review the attachment. One wrong click can cause network outages and downtime.

1

Read the email multiple times.

Look for:

- Spelling mistakes
- Grammar mistakes
- Calls to action
- Threatening language

2

Does the attachment have a link in it requiring an additional step?

In most cases any links are a red flag and should not be clicked without asking a system administrator for input/

3

Does the attachment ask you to enable macros?

DO NOT DO THIS!

Do You Have Doubts?

ASK

Never reply to an email asking for confirmation.

If the email account has been compromised you will get a confirmation that the email is safe to open.

Don't be fooled!

1

Pick up the phone and call the sender to verify the email is legitimate.

2

Ask a system administrator to review the email before opening. It can wait.

3

Assume the email is not legitimate.

ADD AN EXTRA LAYER

Multi-Factor Authentication

PCS

We live in a mobile world

- Your need to be able to sign in from more places than every before.
- Your phone can be the key to making that safe with Multi-Factor Authentication.
- After you sign into a service, an app is launched and you must authorize a signin.
- Same principle as a text with a code.

3rd party service is the easiest way to implement this

- Duo
- AuthAnvil
- Office365
- Onelogin

- It adds a step but only an extra 10 seconds of work to greatly increase security.

DO YOU KNOW WHERE YOU WERE
LAST WEEK? YOUR PHONE DOES!

Turn off location services

Location Service Share

SHARING IS NOT CARING

Location services should be turned off when not in use.

Your phone knows more about you than you realize and you allow it to share that data with advertisers, retailers, hedge funds, and cyberthieves.

1

Location services are needed when you use GPS or look at the whether, otherwise it should be turned off.

2

New York times recently found that over 75 companies use your location data to sell, market, and track you.

3

When you turn off location services you get the added bonus of extra battery life.

FEELING BLUE?

Bluetooth Hacks

Bluetooth is everywhere

ITS BEING EXPLOITED

Almost every device has Bluetooth today and hackers are leveraging as a hacking tool.

- 4 major Bluetooth exploits released in the last year or so.
- It’s a high value target because so many devices are using it.
- Many Bluetooth devices have access to sensitive information or serve as a way into a network.

- Check your devices for unknow Bluetooth devices periodically
- At a minimum you should set a Bluetooth’s visability to ‘OFF’.

MIND BLOWN

Final Thoughts

Continuous Improvement Required

TECHNOLOGY IS NOT "SET IT AND FORGET IT"

Technology changes rapidly and requires daily, monthly, and yearly review.

A business leverages technology is many different ways. As the use of technology advances in your business, it is critical you evaluate each addition a long the way.

1

24/7 Monitoring

- Antivirus/Malware Protection
- Operating System Updates
- File Access
- Employee Access
- Vendor Access
- Backup

2

Annual Risk Assessments

- Penetration Testing
- Employee Education Standards
- Policy Changes

3

Review

- Audit File Permissions
- Audit Group Policy (passwords, drive mapping, group membership)

THANK YOU

Questions?