



ReynCon Educational  
Services & Training

# MOBILE DEVICES & TABLETS



<https://www.reynconsecurity.com>

- **Always Use a Password or PIN**  
Phone, iPad, Droid/Android, Kindle
- **Never Leave Your Cell Phone Unlocked or Unattended**
- **Device Settings**
  - Often the default settings aren't the safest settings
  - Use a pin or biometrics to log into your phone
  - Update and patch OS and applications
- **Be Cautious when Shopping for Applications**  
Applications may contain viruses
- **Download from Trusted Sources**  
iTunes, Amazon, etc.

# SECURITY TIPS | USEFUL LINKS



## **iPhone**

<https://www.zdnet.com/pictures/how-to-secure-your-iphone-from-hackers-snoopers-and-thieves-ios-12-1/>

## **Droid/Android**

<https://www.pcworld.com/article/3187451/6-easy-ways-to-keep-your-android-phone-secure.html>



# Public & Home Wi-Fi

## Public Wi-Fi | Not Always Secure or the best method

- Most cell phone plans offer hotspots on your cell phone as part of your data package – much more secure – has a password assigned specifically to your phone
- Do not do personal banking/paying bills on public Wi-Fi

## Home Wi-Fi | Not Secure by default

- Make sure to change the default password from your internet provider
- Use Phrases – Should be 25+ or longer
  - W3ar3Thech@mp!0n\$myfr!3nd\$1999
- If possible, have a guest access – only allows them to access the internet

# EMAIL SCAMS – Some Things to Watch For



- Do you know the sender?
- Does the email contain attachments, like .exe files, PDF, word, etc.
- Does the email contain an urgent offer with time sensitive deadline (for example “Buy now and get 50% off”).
- Contains misspellings and/or broken English - designed to fool spam filters
- An offer that seems too good to be true
- Subject line and contents do not match
- Contains a request to forward an email to multiple people and may offer a monetary reward
- Links that don't match the intended destination? Use the hover test

# SECURITY QUESTIONS

- **Pick questions that can't be easily found on Facebook, Twitter, Google, LinkedIn, etc.**
  - Maiden Name
  - High School
  - Pets Names
  - Kids Names, etc.
- **Stop doing Social Media quizzes that tend to give away your security answers**
  - **Some people make up answers to their security questions**  
Don't forget the made-up answer 😊
- **Don't write them down**  
Use a password vault

# Passwords & Pin Numbers

Example: Th3Ph@nt0MoftheOp3r@



- **Never Write them on Post-it Notes**  
Or other media close by to devices
- **Use a password vault/manger to store and encrypt all passwords/pin numbers**
- **Include Numbers, Upper/Lower case Letters and Symbols**
- **At Least 9 Characters or More**
- **Use Phrases, Sentences, Lyrics, etc.**
- **Do Not Use**
  - Birthdate
  - Same PIN as ATM or Credit Card
  - Repeating numbers (e.g. 1111 or 2233)
  - Consecutive Numbers (e.g. 123456)

# CREDIT CARD (PCI) & IDENTITY THEFT

- **Shred documents that contain personal and credit card information**
- **Don't write down credit card data**
- **Due Diligence**
  - Pay attention to credit and bank statements – report malicious activity and dispute formally to be most effective
  - Check with credit reporting agencies once a quarter at minimum – You can also request to receive notification anytime your credit is being checked/pulled
- **Use strong passwords and change frequently**
- **Call your CC Fraud department**
  - When Traveling or purchasing high dollar items
  - Set up alerts for all transactions that are Card Not Present(CNP). Set up alerts for some dollar threshold that's slightly above what you normally use the card for.





ReynCon Educational  
Services & Training

# REMOTE WORKERS



- **Avoid public Wi-Fi; if necessary, use personal hotspots or some way to encrypt your web connection – Use a VPN if possible**
- **Keep work data on work computers and separate from your personal computer (if possible)**
- **Never forward work or sensitive data to your personal account**
- **Encrypt confidential data on devices and when sending in emails**
- **Be careful when clicking on links**
- **Lock Laptops/Devices when not in use**
- **Make sure you keep patches up to date**