HOW TO PROTECT YOUR BUSINESS & IPHONE FROM CYBERSECURITY THREATS

Cybercriminals are constantly evolving their tactics and developing new strategies for gaining access to sensitive data stored in companies' servers. To combat this, a robust cybersecurity policy must go beyond simply identifying your company's exposure to risks posed by hackers, scammers, malware and ransomware.

Turning your cybersecurity policy into an ongoing process with committed executive oversight, instead of a one-time project within your IT team, can help ensure you are protected from the latest threats in the digital world.

While there is no one-size-fits-all cybersecurity solution, there are a few universal truths you can implement to help protect against these risks:

1.

DOCUMENT CRITICAL ONLINE BANKING PROCESSES

and approval steps for your company, and don't deviate from them.

SERVICES THAT HELP IDENTIFY FRAUD

Check Fraud Services
- Positive Pay
- Payee Positive Pay
- Reverse Positive Pay

ACH Positive Pay Services
- ACH Debit Block
- ACH Filtering

Requires enrollment in Business Online Banking. Refer to disclosures provided at account opening, the Business Schedule of Fees, and Pro Forma for additional information.

2.

BUSINESS EMAIL COMPROMISES ARE A MASSIVE THREAT TO BUSINESSES.

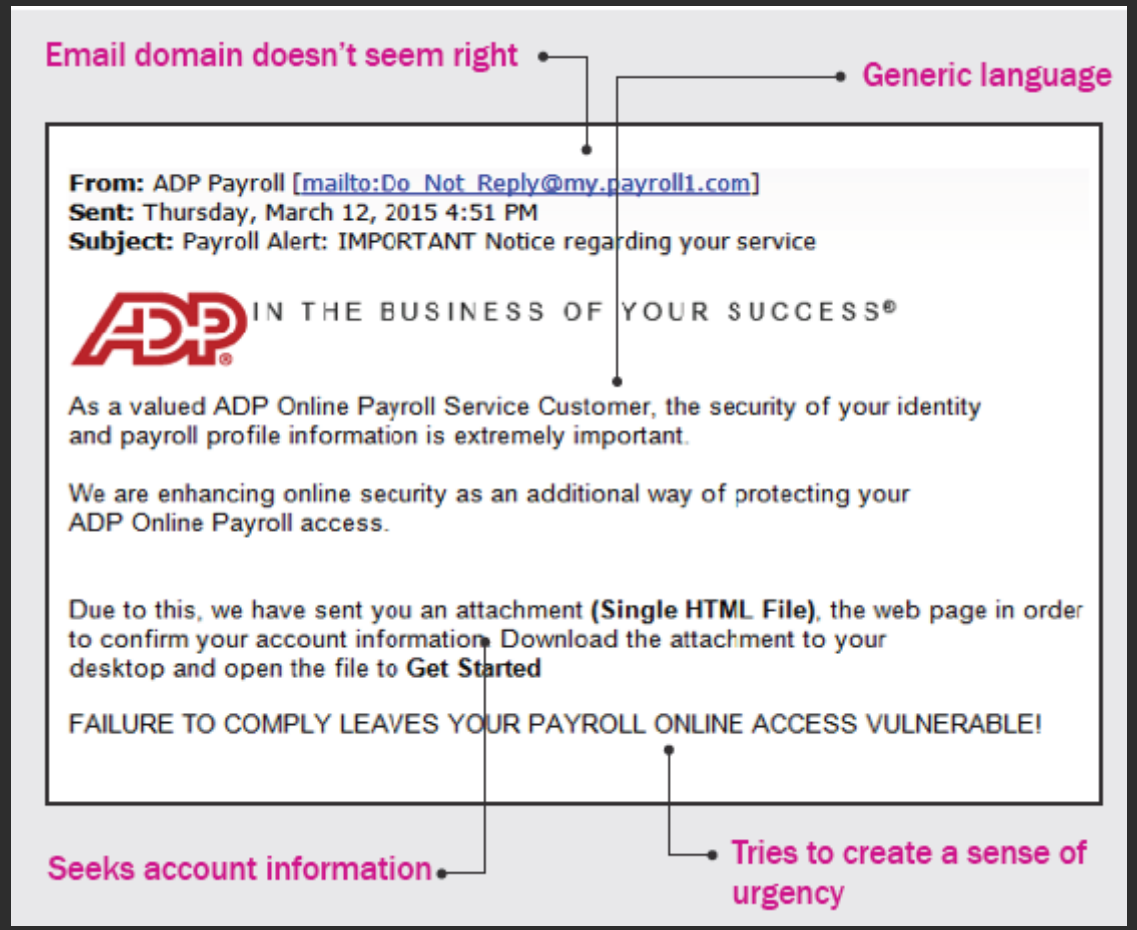
Use the fewest number of dedicated computers for critical online banking functions to avoid corruption introduced through emails or other unsecure sources.

BUSINESS EMAIL COMPROMISE (BEC) SCAMS

- Use email to solicit wire transfers or ACH
- Many impersonate executives or financial officers
- Exploits authority
- Subvert policy / sense of urgency
- Inconvenient timing
- May or may not be initiated by a “Phishing” email

Phishers have stolen billions of dollars in these scams.

COMPROMISE SYSTEM USING PHISHING



TIPS FOR BANK CUSTOMERS

Be mindful of:

- Grammar, spelling and punctuation
- The use of the word “kindly”
- A sense of urgency
- Email addresses that do not match the sender’s name or organization

WHEN IN DOUBT, CALL THE SENDER TO SEE IF IT’S REAL.

TIPS FOR BANK CUSTOMERS

- Always check the sender and verify it is legitimate
- Check reply-to addresses as well
- Just because the sender address looks legitimate doesn’t mean it is
- Speed of notification matters:
  - Wire recoveries attempted after 72 hours have a low recovery rate

LEARN CUSTOMER BEHAVIOR

- Now that they are into the systems…
- Fraudsters look for administrative access.
  - Make changes to gain access and hide there activity
- Learn the organizations behavior
  - Review stored e-mail communication
- Fraudster determines the best way to move funds
  - Looks for any communications discussing funds movement

WHO IS TARGETED FOR THE BEC TRANSACTION?

- Once the hackers reconnaissance is complete and they know the operations of the organization…
- They target and send a BEC e-mail to one of the following targets:
  - Financial officers
  - Employees who can initiate a wire transfer

3.

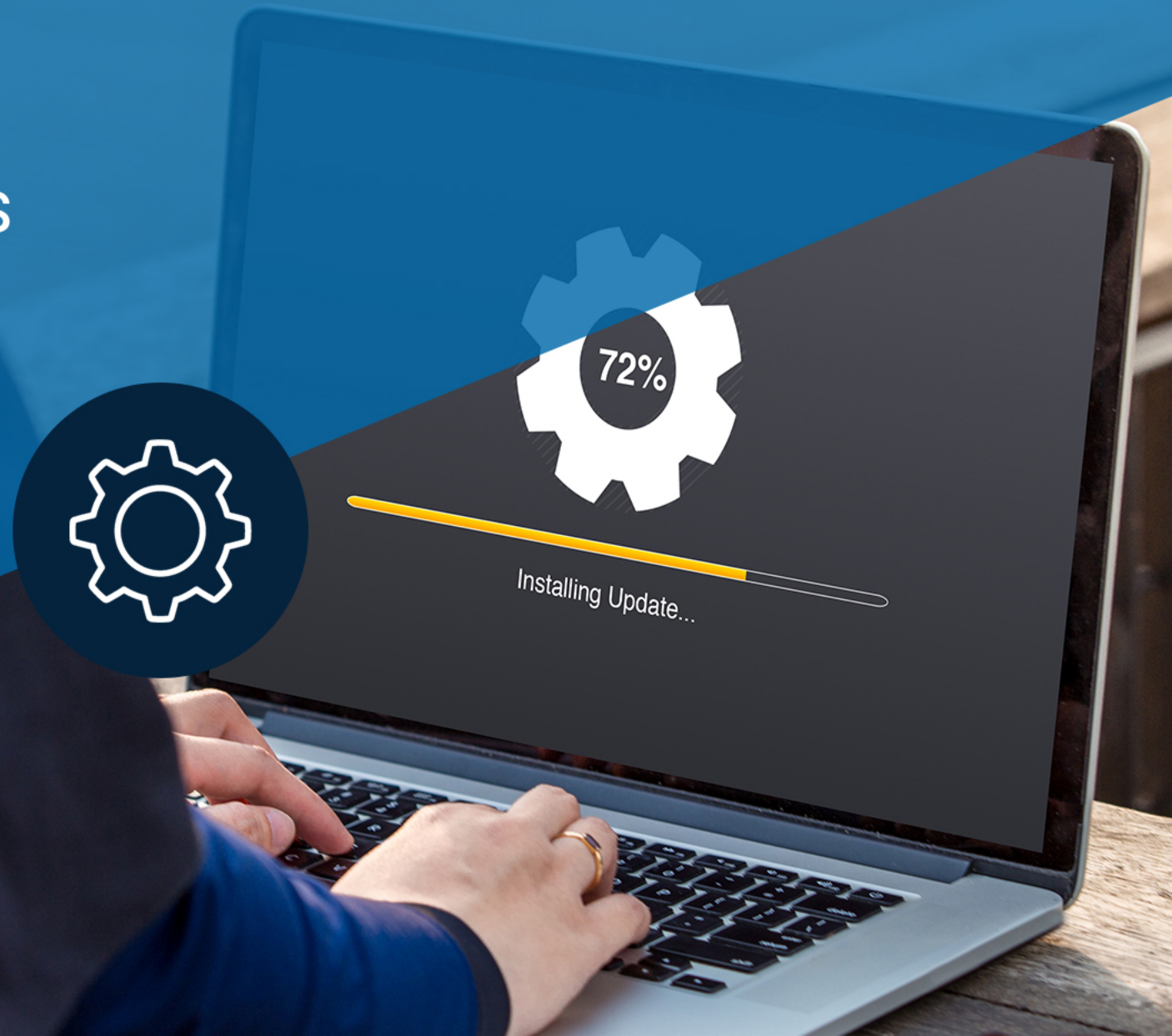
BACKUP CRITICAL DATA REGULARLY and make this task someone's responsibility.

This should be done once a week at a minimum - or as often as makes sense for your operations - with two copies maintained in two different physical locations.

4.

MAINTAIN TOOLS TO PROTECT YOUR COMPUTERS AND SERVERS FROM VIRUSES AND MALWARE.

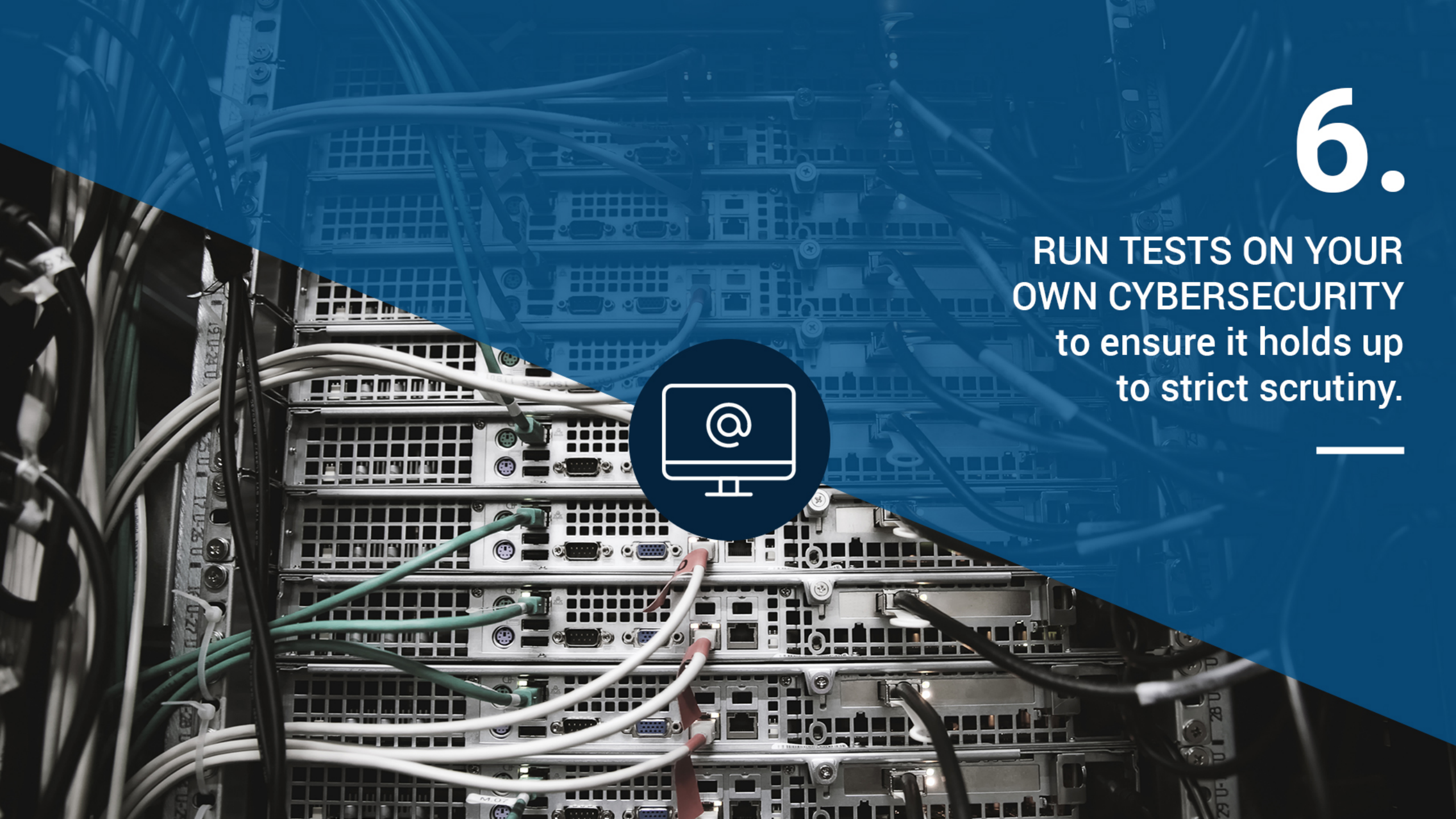
Most importantly, update these tools and systems regularly with updates and patches.



5.

PERIODICALLY REVIEW YOUR CYBERSECURITY PROCESSES with all stakeholders to ensure it is still relevant to your business and industry best practices.

Also review the number of cyber incidents detected to see how frequently they arise.



6.

RUN TESTS ON YOUR OWN CYBERSECURITY to ensure it holds up to strict scrutiny.

Questions?

Protecting Your iPhone

- The typical smartphone contains a lot of personal information, like your credit card numbers, passwords, addresses and other privacy related information.
- To protect that information there are features within your phone that are available to increase your device's security and privacy. Not all these features are turned on by default.
- It is important to address the emerging risks that today's top mobile security threats pose to you and your organization.

Protecting Your iPhone – Terminology

- **iOS:**

This is the Apple operating system of your iPhone. You can find your phone iOS version at Settings> General > About

- **Authentication:**

The is the process or action of verifying the identity of a user. Multi factor authentication. (MFA) Is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence.

- **SIM:**

Subscriber identification module. The SIM card securely stores the international mobile subscriber identity (IMSI) number and its related key which are used to identify and authenticate subscribers on the mobile device.

- **Jailbreaking:**

This refers to a set of technical commands that remove software restrictions imposed by a devices manufacturer. This process may provide the user access to many interesting features that would be unavailable otherwise, but at the same time, it makes them more susceptible to malicious attacks.

Password Basics

Use passphrases or a password manager

- Create long unique passphrases as a best practice
  - Include combo of upper/lower case, special characters, numbers
  - Use a long phrase that is unique to you
- *Example: Apple*
- Use a password manager with two-factor authentication as an alternative option to long passphrases

One iPhone, different applications, different passwords

- Do not use the same passphrase across all your accounts
  - This applies to your phone and PC
- Enable the password auditing feature on your iPhone
  - To find this feature, navigate to Settings> Passwords > Security Recommendations

PIN and Biometrics

Go truly random with your PIN / Passcode

- Easily make your iPhone more secure by creating a random PIN/Passcode
  - Do not use your date of birth, phone number, bank ATM PIN, garage door code, etc.
- Find the Passcode in Settings > FaceID and Passcode

Use biometric authentication on your iPhone

- Use biometric authentication such as fingerprint or facial recognition
  - Adds an extra layer of protection
- Find these features Settings > FaceID and Passcode

MFA and Wi-Fi

Use multi-factor authentication (MFA) whenever possible

- Reduces the risk of someone maliciously accessing your device or accounts
- Use MFA on other accounts as well, including email and other apps when available
- For iPhones, iOS 14 navigate to Settings > <Your Name> Password and Security > Two-Factor Authentication enabled on

Avoid auto-join Wi-Fi networks or hotspots

- Be selective in the Wi-Fi networks or hotspots you join on your phone
- iPhone users should be familiar with the “Ask to Join Network” and the “Auto-Join Hot Spot” features in Settings > Wi-Fi
- Only join a network that was created by someone you know and trust

SIM Card

Protect your SIM

- Create a PIN on your iPhone SIM to reduce hacking if your phone is stolen
- A stolen SIM can result in a hacker resetting and accessing your other accounts
- For iPhone, iOS 14 you can enable your SIM PIN under Settings > Cellular > SIM PIN

Juice Jacking

What is juice jacking?

- USB charging outlets at airports and coffee shops are convenient but can hide a hacking device that installs malware or copies data from your phone as soon as you plug it in. This is known as **juice jacking**.

Protect yourself from juice jacking with a data blocker

- A data blocker is a simple device that sits between the phone's charging socket and the charging device. It blocks data on the connection but allow for charging to occur.
- Use a USB data blocker when charging your phone with shared USB charging outlets.

Backup and Removal of Data

Steps before selling or trading in your iPhone

- Back up your device
- Sign out of iCloud, iTunes & App Store
- Erase Content and Settings
- Contact your carrier to transfer service to new owner if you are not using a SIM card
- Remove your old device from your list of trusted devices
- Keep in mind - when you erase your iPhone, iPad, or iPod touch, the Find My [device] and Activation Lock features are turned off

Backup and Removal of Data

iPhone step by step for backup and data removal

- **To back up your device**
  - Go to Settings > [your name] > iCloud > iCloud Backup
- **Sign out of iCloud, iTunes & App Store**
  - iOS 10.3 or later, tap Settings > [your name] > Sign Out. Enter your Apple ID password and tap Turn Off.
  - iOS 10.2 or earlier, tap Settings > iCloud > Sign Out > Tap Sign Out again >tap Delete from My [device] and enter your Apple ID password > Settings > iTunes & App Store > Apple ID > Sign Out
- **Erase Content and Settings**
  - Settings > General > Reset > Erase All Content and Settings
    - If you turned on Find My [device], you may be asked to enter your Apple ID and password. If asked for your device passcode, enter it > Erase [device]

Jailbreaking and Applications

Do not use a jailbroken iPhone or sideload apps

- Jailbreaking: allows a user to run non-iPhone approved applications by sideloading those applications
    - Sideloading: downloading apps from outside the Apple App Store
- Users go through a complex process to jailbreak their iPhone to avoid paying for applications

Use fewer apps

- Apps increase the ‘attack surface’ of your phone and opportunities to invade your privacy
- Delete apps you do not use
    - Want to go the extra mile? Remove social media apps from your iPhone, as those applications typically collect information about you, your iPhone’s usage and your location. Instead, use the phone’s browser to access social media sites

Notifications and MAMS

Be aware of notifications containing private information

- Update the notification settings on your phone to show notification previews ONLY when your phone is unlocked
  - Example ~ if you're trying to reset a password on a website, a code may arrive as a notification on your phone. If your phone has been stolen, you just gave the thief access to reset the password.
  - View iPhone notifications in Settings > Notifications

Consider a Mobile Access Management (MAM) for your business

- MAMs build a secure container around your business applications and data to keep them separate and protected from employees' data and applications
- Use a MAM platform to distribute your company's private apps to increase security

Applications and Permissions

Beware of fake mobile applications

- Mobile apps allow a pathway into your device that is not necessarily developed or easily controlled by the phone manufacturer
- Malicious apps can access your personal information or trick you into entering personal data
- Double-check the legitimacy of the app before downloading and read reviews on the app

Review your app permissions

- Understand what permissions you grant your phone applications
  - Go to Settings > Privacy > Choose category
- Is the app worth the risk?
  - Permissions are incredibly powerful. Make sure the risk of losing your privacy by granting permissions is worth the benefit the application provides
- Granting permission to information is a one-way deal. Your information does not remain solely in the hands of the application provider

Protecting Your iPhone

Allow automatic iOS updates

- Allow “Automatic Updates” and “Install iOS Updates” to your iPhone to ensure more up to date security updates are installed
  - iPhone > Settings > General > Software Update
- Applications updates also can include security enhancements, so accept those updates as soon as they are released

Disable "Load Remote Images" in email settings

- Hidden trackers may exist in images embedded in emails, allowing the sender to track whether you’ve opened the email and other information
- When you click on an email, your phone can then share details about your device with the server such as browser version, what operating system you’re using and sometimes your location
- On an iPhone go into Settings > Mail, set the switch next to "Load Remote Images" to the off position

Protecting Your iPhone Summary

Most important ways to protect your iPhone and your privacy

- ✓ Use passphrases and don't reuse your passphrases on different accounts
- ✓ Create a unique PIN/Passcode in Settings > FaceID and Passcode
- ✓ Allow "Automatic Updates" and "Install iOS Updates" to your iPhone
- ✓ Use MFA features under Settings > <Your Name> Passwords and Security.
- ✓ Review your app permissions

Also helpful

- ✓ Enable Biometrics Face ID in Settings > FaceID and Passcode
- ✓ Protect your iPhone from "juice jacking". Use a USB data blocker (available on Amazon) when charging your phone with shared USB charging outlets
- ✓ Before selling or trading in your iPhone backup your iPhone and delete data following the Apple recommended procedure.
- ✓ Don't mess with jailbroken phones
- ✓ Businesses allowing employees to access company email and data using their personal phone should use a Mobile Device Manager