Safety and Security

April 2015

Protecting your smartphone and your data

Set a passcode on your smartphone

For some smartphone models:

1. Go to Settings.
2. Tap ID & Passcode.
3. Set a 4-digit passcode.

For other smartphone models:

1. From the home screen, tap Apps.
2. Swipe to, then tap Settings.
3. From the "My device" tab, tap Lock screen.
4. Tap Password.
5. Enter the desired password, then tap Continue.
6. Confirm your new password, then tap OK.

Change a passcode on your smartphone

For some smartphone models:

1. Tap Passcode.
2. Enter your 4-digit passcode.
3. Tap Change Passcode.
4. Enter your new Set a 4-digit passcode.

For other smartphone models:

1. From the home screen, tap Apps.
2. Swipe to, then tap Settings.
3. From the "My device" tab, tap Lock screen.
4. Tap Screen lock.
5. Enter your password, then tap Continue.
6. Tap the desired new lock screen.

A sampling of free security apps

- **Anti-Theft Alarm:** Triggers a siren when a phone is moved or when the charger is disconnected.
- **AT&T Mobile Locate:** Lock, back up and wipe your device and restore your data remotely.
- **Google Authenticator:** Creates a two-step verification code on phones that helps prevent thieves from accessing accounts and other information.
- **Hidden Anti Theft:** Tracks the location of iPhones and has the ability to covertly take real time photos from the phone so users can see who has it and where they are.
- **KeepMyIdentities:** Increase the security of Microsoft accounts by generating random passcodes and securely storing users' login information.
- **Keeper:** Protects users by encrypting login, financial and other digital information and using two-factor authentication.
- **Lookout:** Locate lost or stolen devices, set off an alarm, download contacts to a new device and more.

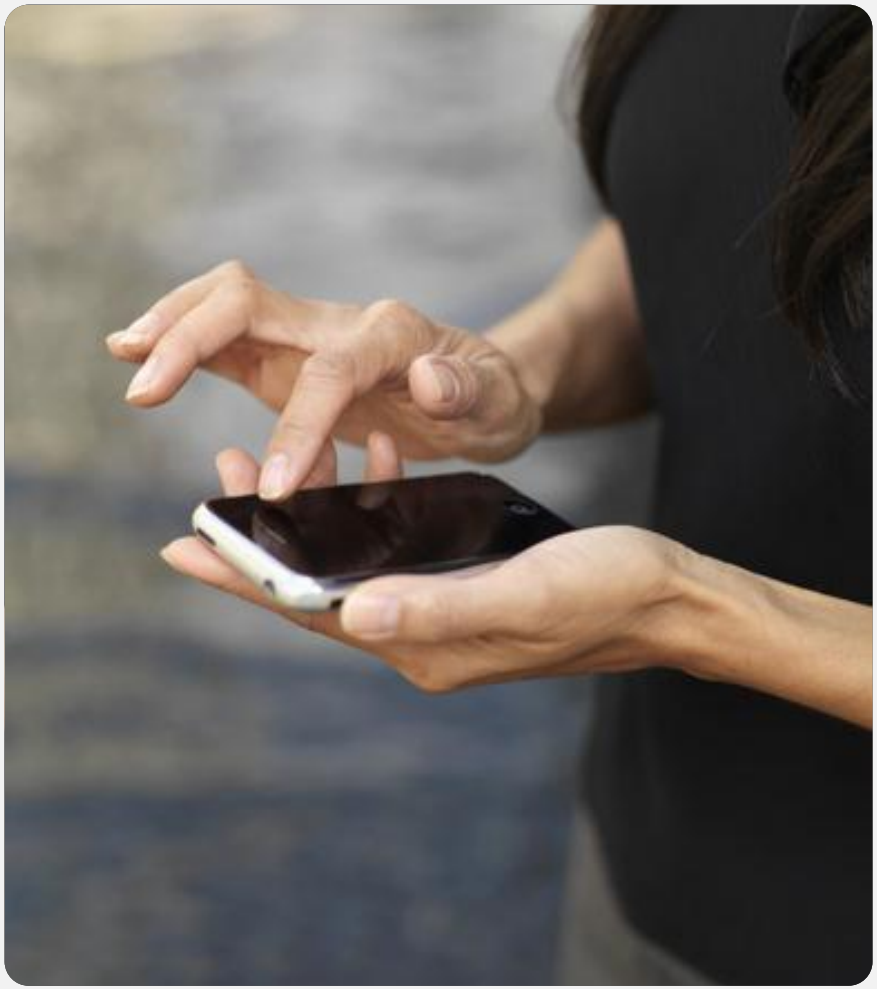
Tips for protecting your information

- Back up your data
- Be careful with sensitive information when using public Wi-Fi

How to protect yourself when using an unsecure Wi-Fi connection

- **Avoid connecting to suspicious Wi-Fi networks.**
- **Install a mobile antivirus and security app from your device app store and update its settings to automatically scan for viruses.**
- **Select apps that use encryption and are well rated in your app store.**
- **Connect to a Virtual Private Network (VPN) for maximum security protection.**
- **Ensure your Web-based email is secure.**

Password Tips

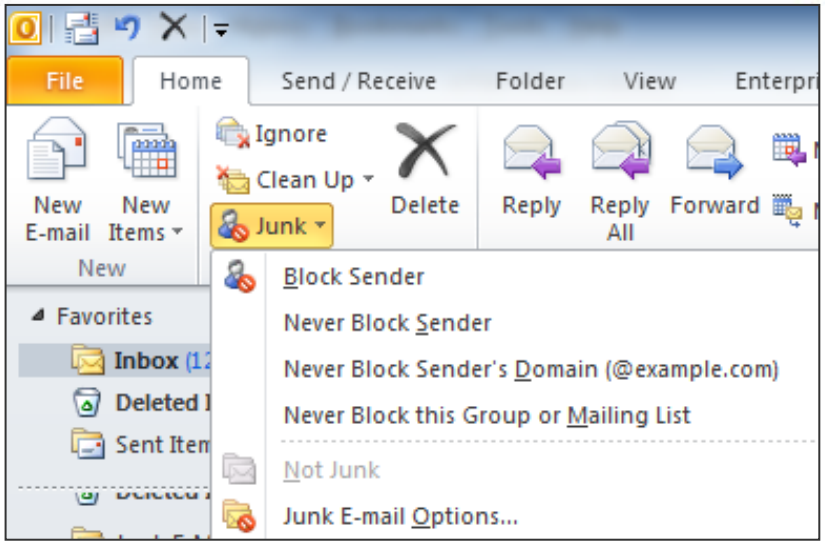


- Long and strong (when possible).
- Mix of upper and lowercase letters, numbers and symbols.
  No sharing!
- Make your password unique to your life and not something that is easily guessed
- Have a different password for each online account.
- If you write down your password, store it in a safe place away from your computer.
- Change your password several times a year.

Scams and Shams

Email Fraud/Phishing

1. **Read your emails carefully**: make sure you **know the sender** and **be suspicious** of any email that asks for your personal or financial information.
2. **Be very cautious when downloading any attachments** or files from an email, unless you know and trust the sender.
3. **Pay close attention to the URL** to see if it's organized in an unusual way.
4. **Look for poor grammar or spelling**.
5. **Check for a lack or incorrect use of trademarked symbols**.
6. **Be wary of links that lead to unfamiliar pages**.
7. No reputable institution or organization will ask you to email them sensitive information (financial, health, etc.). **Do not hit the reply button and send the information**.



Government Agency Scam

What it is:

Someone calls you claiming to be a **government agency**, such as the IRS, and **asks you to provide sensitive personal information**. They often threaten you with legal action if you don't.

What you should do:

- **Do not engage – hang up immediately.**
- If you suspect that such an obligation exists, **contact the government agency at their published phone number**(s) to verify.
- For the IRS-related scam:
  - For more information: http://www.irs.gov/uac/Newsroom/IRS-Repeats-Warning-about-Phone-Scams
  - To report the scam to the Treasury Inspector General's Office: http://www.treasury.gov/tigta/contact_report_scam.shtml

PC Technical Support Scam

What it is:

Someone contacts you **claiming to be a computer technician** with a technical support company or affiliated with your internet service provider. They may tell you **they have detected viruses or malware** on your computer or offer a free security scan on your computer. Once you provide them with remote access to your computer **they either attach malware which can steal your sensitive data or "lock" your computer** and demand payment to "unlock."

What you should do:

- **Never provide remote access to your computer** under these circumstances.
- In all cases, **never engage such services without first verifying** that the company is in fact genuine.
- For more info: http://www.consumer.ftc.gov/articles/0346-tech-support-scams.

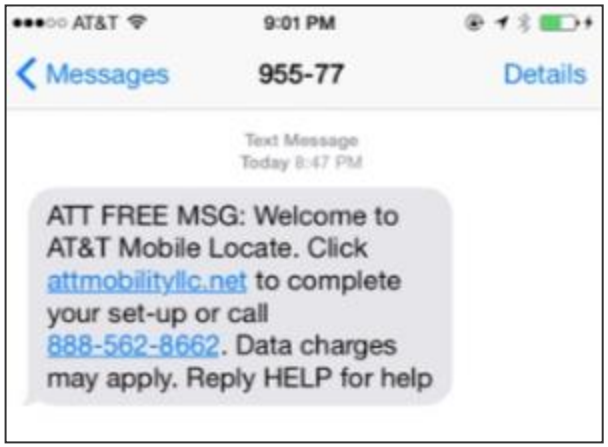
Fake Website Phishing Scam

What it is:

You receive a **call, text or email enticing you to visit a website that appears to have an affiliation with a well-known company**. For example, once at a fraudulent AT&T website, you are prompted to log in with your MyATT account credentials. The **fraudster then uses the information obtained from the fake site** to log into your account and **make changes to the account or place orders**.

What you should do:

- Ignore it.
- Never use your AT&T account information to log into any website other than the AT&T website listed on your statement.
- Customers can report this activity to AT&T at abuse@att.net. For unwanted text messages, forward the message to short code 7726 (SPAM) and AT&T will investigate.
- If you already have been a victim of phishing, you should file a complaint with the Internet Crime Complaint Center (IC3) at www.IC3.gov.



“One-Ring” Callback Scam

What it is:

Fraudsters use call generators to **place calls to a large volume of phone numbers**. The calls typically ring once. The **number** displayed on the recipient’s caller ID **is a high-cost international number**, usually located in the Caribbean. If you call the number back you’re greeted with a message designed to keep you on the line, such as “Hello, you have reached the operator, please hold.” **The longer you stay on the line, the more revenue fraudsters generate**.

What you should do:

- Do not answer or return calls from numbers you do not recognize or initiate a return call. You will not be charged for receiving the calls.
- Companies that do not conduct business with companies in the above-mentioned countries may want to consider blocking these area codes to avoid this type of charge.
- If you have been victimized by this scam, you can file a complaint at www.ftc.gov and www.IC3.gov.