



# Mobile Security Best Practices, Tips and Insights

Office of the Chief Information Officer

***NASA IT Vision:** The NASA IT Organization is the **very best** in government*

**Shawn Postich**  
**ETADS**  
**June 27, 2012**

# About ETADS

- **The Emerging Technology and Desktop Standards (ETADS) program** was established at the Glenn Research Center in 1996 to support the [NASA's Office of the Chief Information Officer](#). It consists of a state-of-the-art testbed facility, the Emerging Technology Assessment Facility (ETAF), and an experienced and diverse staff capable of understanding both the technical intricacies of modern operating environments and the complexities associated with NASA-wide implementations.
- The ETADS group is responsible for establishing and maintaining hardware, software, and security configuration standards for end user computing devices. It produces NASA's basic interoperability standards (NASA-STD-2804 and NASA-STD-2805), and provides leadership in the areas of desktop smartcard integration and compliance with federal computer security configuration regulations, such as the Federal Desktop Core Configurations (FDCC).

## Guiding Principles:

- End-user devices and services will enable NASA's mission by facilitating information sharing across the Agency to enhance and accelerate decision-making.
- NASA end users will be empowered to select devices that best meet mission requirements without sacrificing interoperability.
- NASA will promote Agency-wide standardization of hardware, software, and security configurations, and system management processes to maximize the cost-effectiveness of its IT initiatives.
- NASA will ensure the confidentiality and integrity of the data residing on and transferred between end-user devices.

<https://etads.nasa.gov/>



# About Shawn Postich

- Started in IT in 1992
- Supporting NASA IT since 1994
- Directly supporting and contributing to NASA's security posture since 1999.
- Multiple certifications, accreditations, awards and acknowledgements.



# Agenda

- **The Mobile Landscape**
- **Current Mobile Risks**
- **Emerging Risks**
- **Lost Mobile Device Statistics**
- **10 Easy Steps to Protect You and Your Device**
- **Additional Safeguards**
- **Closing Thoughts**
- **Questions**

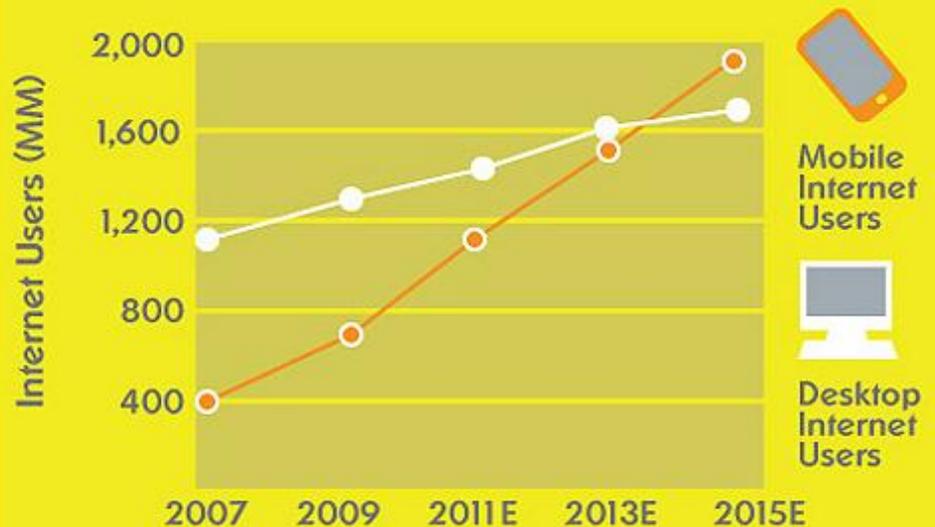
# The Mobile Landscape



📱 How fast is mobile internet growing?

**By 2014, mobile internet should take over desktop internet usage**

Global Mobile vs. Desktop Internet User Projection, 2007 - 2015E



# The Mobile Landscape

📱 How much do people use their mobile phones? 📱 What do people use their mobile phones for?



On average, Americans spend **2.7 hours** per day socializing on their mobile device



That's over **twice** the amount of time they spend **eating**, and over **1/3** of the time they spend **sleeping** each day

LOL

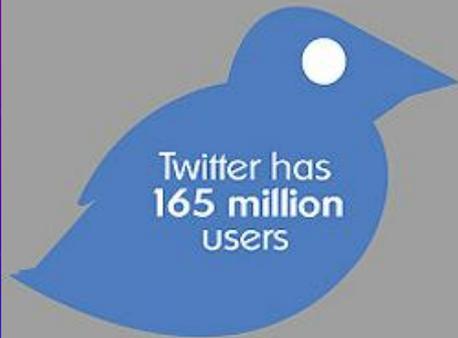
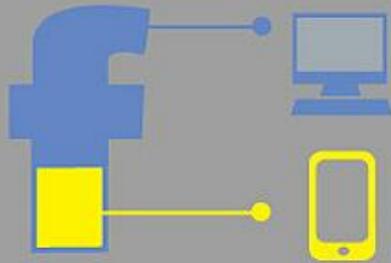


Zzzz... lol



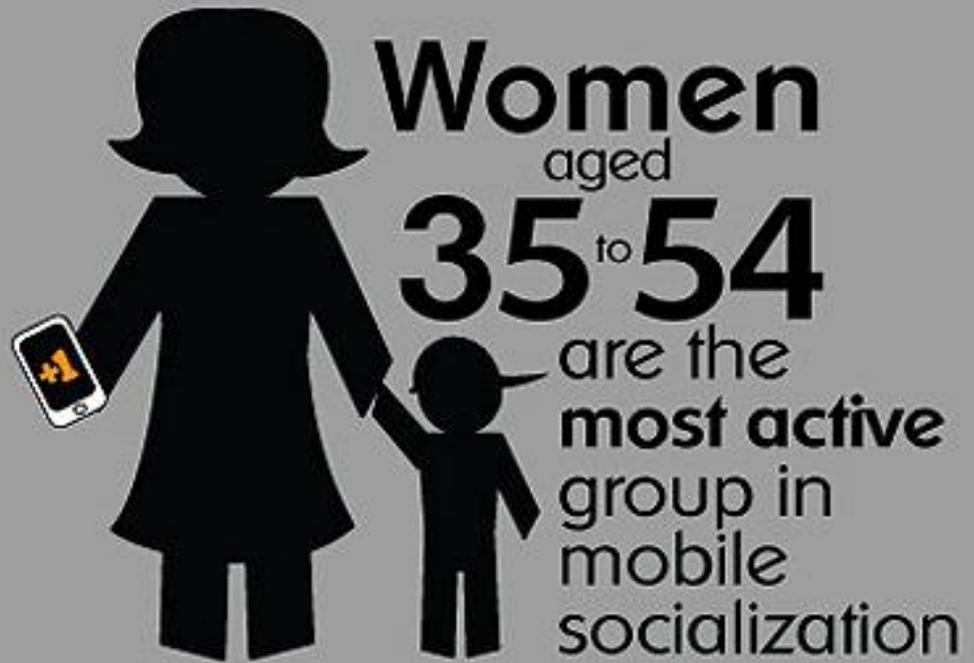
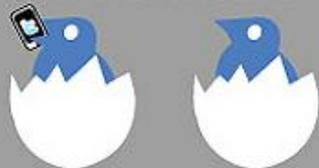
# The Mobile Landscape

Over 1/3  
of Facebook's  
600 million+  
user base uses  
Facebook  
Mobile



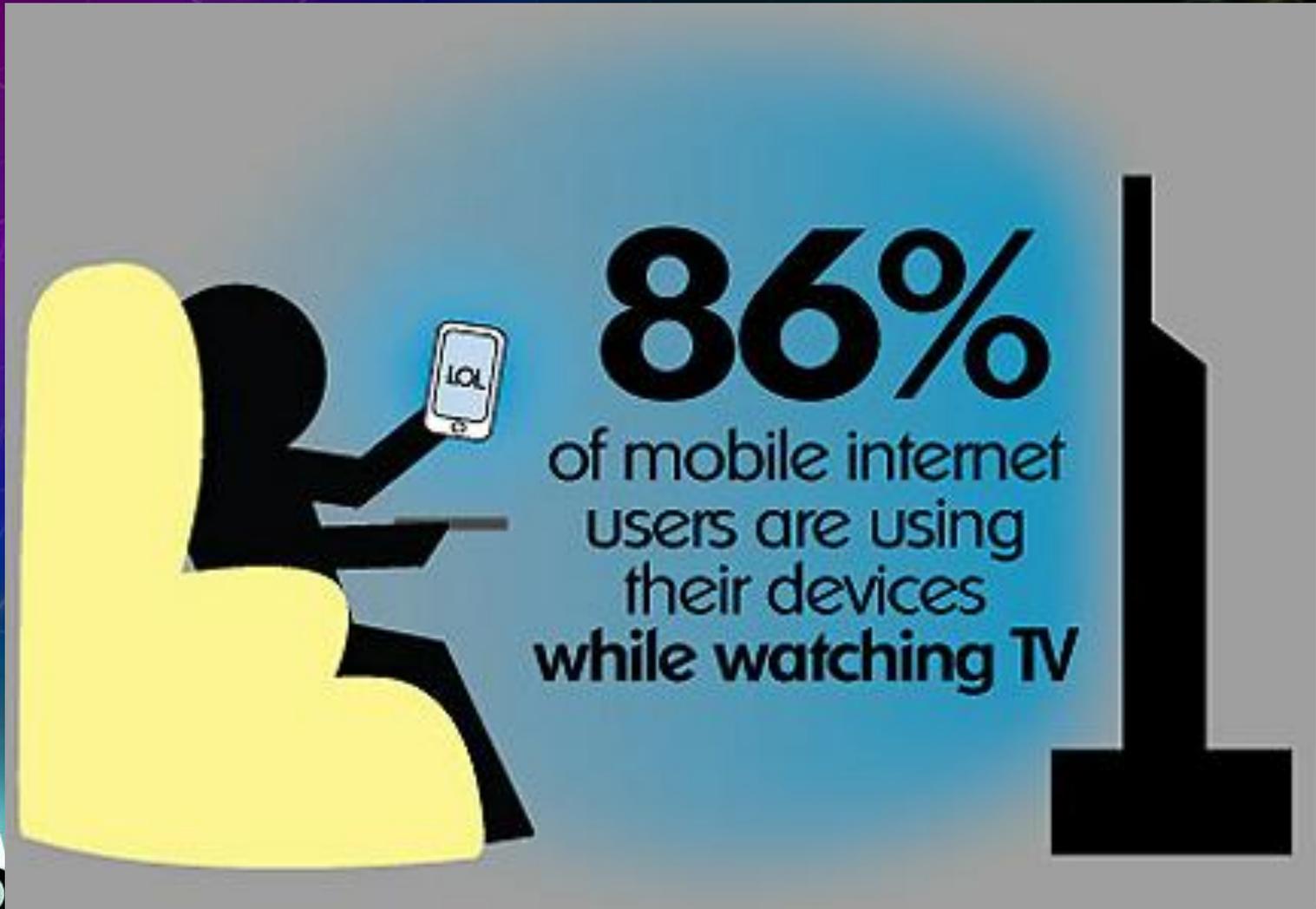
Twitter has  
165 million  
users

50% of them use  
Twitter Mobile



Women  
aged  
**35 to 54**  
are the  
most active  
group in  
mobile  
socialization

# The Mobile Landscape



# Where Thing\$ Are Heading...

## THE GROWING MOBILE PAYMENTS MARKET

Mobile payment transactions already total \$240 billion annually, but that's just the tip of the iceberg. Juniper Research reports that the market will grow 2x to 3x in the next 5 years.



### By 2013:

Sales of NFC equipped phones will exceed

**\$75 billion.**



**1 in 5** cell phones worldwide will use NFC technology.

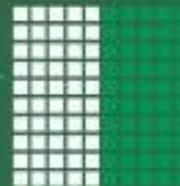


### By 2014:

NFC transactions alone will approach

**\$50 billion.**

Google predicts that **50%** of cell phones will use NFC technology.



### By 2015:

The value of all mobile money transactions is expected to reach

**\$670 billion.**

Digital goods will make up nearly 40% of this market. Asia, Western Europe and North America will be responsible for **75% of all mobile payment transactions.**

# So what do we know...

We use our mobile devices **longer**

We use our mobile devices to do **more**

We share **everything**

We'll be **buying even more** with our mobile devices

We probably **aren't paying attention** when we use our mobile devices

***But, this is not a good time to grow complacent...***



Source: [Lookout.com](http://Lookout.com)

# The Risks We Face...

**Malware:** Software that is designed to engage in malicious behavior on a device. For example, **malware can commonly perform actions without a user's knowledge**, such as making charges to the user's phone bill, sending unsolicited messages to the user's contact list, or giving an attacker remote control over the device. Malware can also be used to steal personal information from a mobile device that could result in identity theft or financial fraud.

**Spyware:** **Designed to collect or use data without a user's knowledge or approval.** Data commonly targeted by spyware includes phone call history, text messages, location, browser history, contact list, email, and camera pictures.

**Privacy Threats:** May be caused by applications that are not necessarily malicious (though they may be), but **gather or use more sensitive information** (e.g., location, contact lists, personally identifiable information) than is necessary to perform their function or than a user is comfortable with.

# The Risks We Face (cont.)...

**Vulnerable Applications:** *Contain software vulnerabilities that can be exploited for malicious purposes. Such vulnerabilities can often allow an attacker to access sensitive information, perform undesirable actions, stop a service from functioning correctly, automatically download additional apps, or otherwise engage in undesirable behavior. Vulnerable applications are **typically fixed by an update** from the developer.*

**Phishing Scams:** *Use web pages or other user interfaces designed to **trick a user into providing information** such as account login information to a malicious party posing as a legitimate service. **Attackers often use email, text messages, Facebook, and Twitter to send links to phishing sites.***

**Drive By Downloads:** ***Automatically begin downloading an application** when a user visits a web page. In some cases, the user must take action to open the downloaded application, while in other cases the application can start automatically.*



# The Risks We Face (cont.)...

**Browser Exploits:** *Are designed to **take advantage of vulnerabilities in a web browser or software that can be launched via a web browser** such as a Flash player, PDF reader, or image viewer. Simply by visiting a web page, an unsuspecting user can trigger a browser exploit that can install malware or perform other actions on a device.*

**Network Exploits:** *Take advantage of software flaws in the mobile operating system or other software that operates on local (e.g., Bluetooth, Wi-Fi) or cellular (e.g., SMS, MMS) networks. **Network exploits often do not require any user intervention**, making them especially dangerous when used to automatically propagate malware.*

**Wi-Fi Sniffing:** *Can compromise data being sent to or from a device by taking advantage of the fact that many **applications and web pages do not use proper security measures**, sending their data in the clear (not encrypted) so that it may be easily intercepted by anyone listening across an unsecured local wireless network.*



# Examples of The Risks We Face

**Gaming Apps**

 BubbleBuster, repackaged with DroidDream Light

 Chess, repackaged with DroidDream

 Spiderman, repackaged with DroidDream

**Utility Apps**

 Battery Saver app, repackaged with GGTracker

 Scientific Calculator app, repackaged with DroidDreamLight

**Porn Apps**

 Porn app, repackaged with GGTracker

lookout



# What To Expect Next:

Malware that acts as a botnet, exposing an array of remotely controlled device capabilities.

Abuse of premium-rate text messages

- Notify your carrier
  - Install call blocking apps
  - iOS “Blacklist”
  - Android “DroidBlock, CallFilter”
- Consider Google Voice

Targeted attacks aimed at gathering sensitive data for commercial or political purposes

Financial fraud as more mobile finance and payment apps emerge



Source: [Lookout.com](http://Lookout.com)

## And, More Bad News....

- **Before you finish** reading this sentence, **someone will lose** their mobile device.
- They have a **50/50 chance** of getting it back.
- When found, **someone will try** to access its content.

# Cities with The Highest Mobile Loss Rates

1. Philadelphia
2. Seattle
3. Oakland
4. Long Beach
5. Newark
6. Detroit
7. **Cleveland**
8. **Baltimore**
9. New York
10. Boston
11. Milwaukee
12. Atlanta
13. **Houston**
14. Tampa
15. Fort Lauderdale
16. **San Francisco**
17. Fort Worth
18. **Orlando**
19. **Sacramento**
20. Chicago
21. San Diego
22. San Antonio
23. Austin
24. Pittsburgh
25. Salt Lake City
26. Indianapolis
27. **Los Angeles**
28. Charlotte
29. **Washington**
30. **Nashville**

# Where You're Most Likely To Lose Your Phone:

10. Purse

5. School

9. Restaurant / Bar

4. Bus or Subway

8. Roof of Your Car

3. Airplane

7. Changing Room

2. Taxi

6. Airport Security

1. Pool

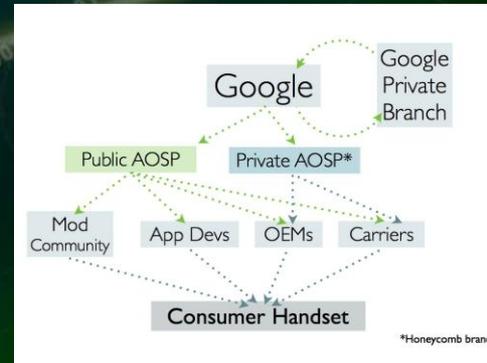
# 10 Easy Steps To Protect Your Device & You

1. Set a password for your phone and voicemail.
  - » IOS: **Settings > General > Passlock**
  - » Android: **Settings > Security > Screen lock**
    - **Don't use a swipe pattern or facial recognition.**
2. Turn on autolock
  - » IOS: **Settings > General > Auto-Lock > Set time to 5 minutes**
  - » Android: **Settings > Sound and Display > Screen Timeout**
3. Do not use public Wi-Fi at airports or coffee shops for accessing sensitive information. If possible use your phone carrier's network or a VPN connection instead.
4. Disable Bluetooth if you do not use it. If you do use a Bluetooth device, always pair your Bluetooth device with your smartphone.
5. Choose your apps carefully.
  - » **Research, Review (and Remove)**
  - » **Android: When installing apps, consider carefully the granting of permissions**



# 10 Easy Steps To Protect Your Device & You

1. Do not click on text message links sent by anonymous senders.
2. Do not Jailbreak your phone. Jailbreaking will remove security features on your phone which can expose you to data theft and loss of privacy.
3. Install the latest patch and OS updates when they are available.
  - » Android device shelf life is typically short (and possibly slow to arrive)



Version	Codename	API Level	Distribution
1.5	Cupcake	3	0.3%
1.6	Donut	4	0.6%
2.1	Eclair	7	5.2%
2.2	Froyo	8	19.1%
2.3 - 2.3.2	Gingerbread	9	0.4%
2.3.3 - 2.3.7		10	64.6%
3.1	Honeycomb	12	0.7%
3.2		13	2%
4.0 - 4.0.2	Ice Cream Sandwich	14	0.4%
4.0.3 - 4.0.4		15	6.7%

4. Backup your data and enable auto-erase in case your phone is ever lost or stolen.
5. Leave your phone at home if you are traveling abroad and purchase a prepaid phone to make overseas calls.

# Additional Safeguards

## ▪ Encrypt your phone:

- IOS: It's on by default
- Android: (ICS) Settings > Personal > Security > Encryption > Encrypt phone.

## ▪ Enable a *Find My Phone* feature:

Great for finding your kids!

IOS:



- Open a web browser
- Navigate to: <https://www.icloud.com>
- Sign in
- Click “Find My Phone”

Android:

Download “LookOut – Free Version”

<https://www.mylookout.com/>



# Additional Safeguards

Consider **repeating a digit** when you set your passlock:



## Huh? But Why?

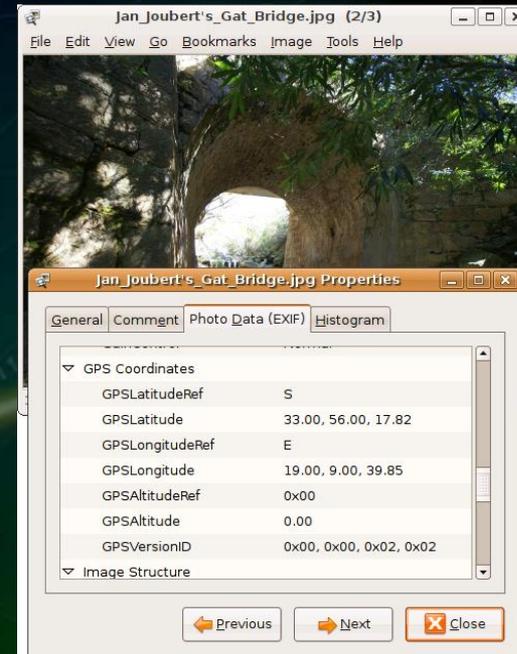
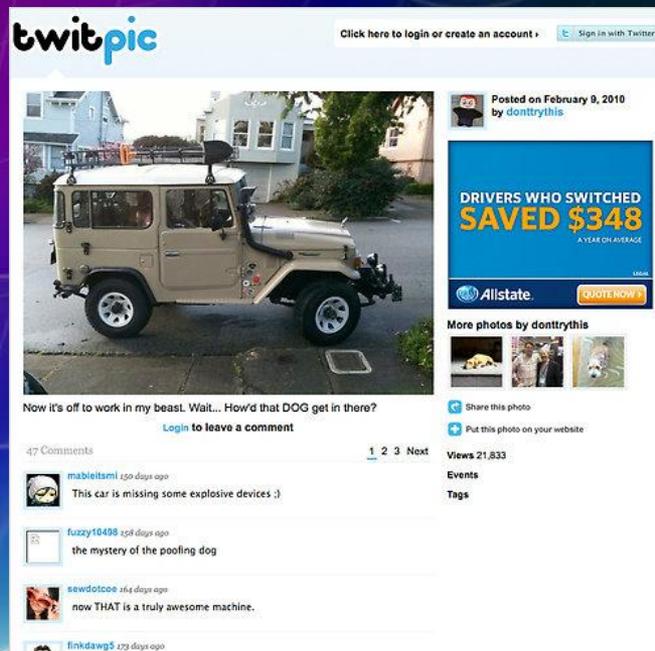
**Multinomial Coefficient:**  
*The multinomial coefficient is calculated as the total number of permutations divided by terms that account for non-distinct or repeated elements. If an element appears  $k$  times (i.e. has a multiplicity of  $k$ ), then the factor to divide by is  $k!$*

**Caution: Only repeat one digit.**

# Additional Safeguards

## Understand Geotagging:

Geotagging is the process of adding geographical identification to photographs, video, websites and SMS messages. *It is the equivalent of adding a 10-digit grid coordinate to everything you post on the internet.*



## Be careful what you Tweet:

“MythBusters” host Adam Savage posted this geo-tagged picture of his car (parked in front of his home) and Tweeted “Now it’s off to work.”

“Just shot a 33 on the front 9!”

“Should I order dessert? YUMMMMMY!”

# Additional Safeguards

## How to Disable Geotagging:

### IOS:



### Android:



# More Precautions

- Check your bill regularly
  - » There's an app for that!



- Backup your data and encrypt it
  - » iTunes - Summary Tab – Options – Encrypt iTunes Backup



- Beware shoulder surfers (Really!)
  - » consider privacy filters



# Additional Safeguards

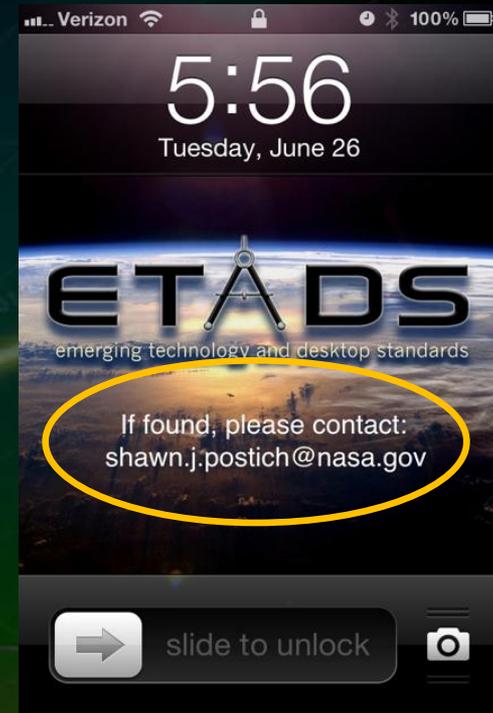
## ■ Personally Brand Your Phone:

- » Here's how:
- » From your PC open the image you want to use
  - Mac: Preview – Tools - Annotate – Add Text
  - Windows: Paint – Text Icon – Add Text
- » Save image to PC - email it to yourself
- » Save to mobile gallery, select as lock screen

## ■ Before recycling your phone:

- » Remove the SIM card
- » Wipe the data
  - IOS: Settings – General – Rest – Reset All Content and Settings
  - Android: Applications - Settings – Privacy – Factory Data Reset
    - Manually wipe and remove the SD Card.

(Pictures have a nasty habit of sticking around)



# Closing Thoughts...

- iOS 6 - expected Fall 2012
  - » Guided Access: “Guided Access makes it possible for parents and teachers to disable hardware buttons on an iOS device, so that the device can be locked into a single app.”
- Mobile is empowering
- Mobile is also an inviting field of opportunity for bad guys
- Best practices are like car insurance
- You have the tools....

# Questions

???

# Contacts

## ***Emerging Technology and Desktop Standards***

Service Executive: [John Sprague](#)

ETADS Program Manager: [Irene Wirkus](#)

Author and Presenter: [Shawn Postich](#)

For more information: <https://etads.nasa.gov/>

## ***IT Security Awareness Training Center***

Program Manager: [Rich Kurak](#)

For more information: [ITSATC@lists.nasa.gov](mailto:ITSATC@lists.nasa.gov)

[http://www.grc.nasa.gov/WWW/CIO/ec\\_itsat/index.htm](http://www.grc.nasa.gov/WWW/CIO/ec_itsat/index.htm)



# Next IT Security WebEx

## Threats and Dangers of Social Networking

Jeremy Conway, Managing Partner at SudoSecure

Tuesday, July 17, 2012

11:00 am CDT

- To sign up,
  - » Email: [ITSATC@lists.nasa.gov](mailto:ITSATC@lists.nasa.gov)
  - » Subject: WebEx – Social Networking
  - » Please include name, Center, & contact information



# Resources

ETADS White Papers

<https://etads.nasa.gov/research/whitepapers/>

ETADS Research and Assessments

<https://etads.nasa.gov/research/>

ETADS IOS and Android Benchmarks

<https://etads.nasa.gov/ascs/benchmarks/>



# References

- [Mindyourdiscussions.com](http://Mindyourdiscussions.com)
- [Smartinsights.com](http://Smartinsights.com)
- [Lookout.com](http://Lookout.com)
- [TalkAndroid.com](http://TalkAndroid.com)
- [Pureinfographics.com](http://Pureinfographics.com)
- [Symantec.com](http://Symantec.com)
- [Wired.com](http://Wired.com)
- NASA ARC IT Security Newsletter (May 2012)
- [Mashable.com](http://Mashable.com)
- [Schneier.com](http://Schneier.com)

# References

- [Mindyourdiscussions.com](http://Mindyourdiscussions.com)
- [Smartinsights.com](http://Smartinsights.com)
- [Lookout.com](http://Lookout.com)
- [TalkAndroid.com](http://TalkAndroid.com)
- [Pureinfographics.com](http://Pureinfographics.com)
- [Symantec.com](http://Symantec.com)
- [Wired.com](http://Wired.com)
- NASA ARC IT Security Newsletter (May 2012)
- [Mashable.com](http://Mashable.com)
- [Schneier.com](http://Schneier.com)

## References

- [Theunderstatement.com](http://Theunderstatement.com)
- [Infoworld.com](http://Infoworld.com)
- [Lookout.com](http://Lookout.com)
- [Extremetech.com](http://Extremetech.com)
- [Android.com](http://Android.com)