



ONLINE SAFETY

Christopher Burgess
CEO, Prevendra, Inc.

Prevendra, Inc.
PO Box 974
Woodinville, WA 98072
info@prevendra.com

 425-318-7860  [@BurgessCT](https://twitter.com/BurgessCT)
 [@SafetySeniors](https://twitter.com/SafetySeniors)



AGENDA

Online Safety

- * Demographics
- * What are we doing online?
- * Threats
- * Solutions:
 - * Keep your device safe
 - * Keep yourself safe

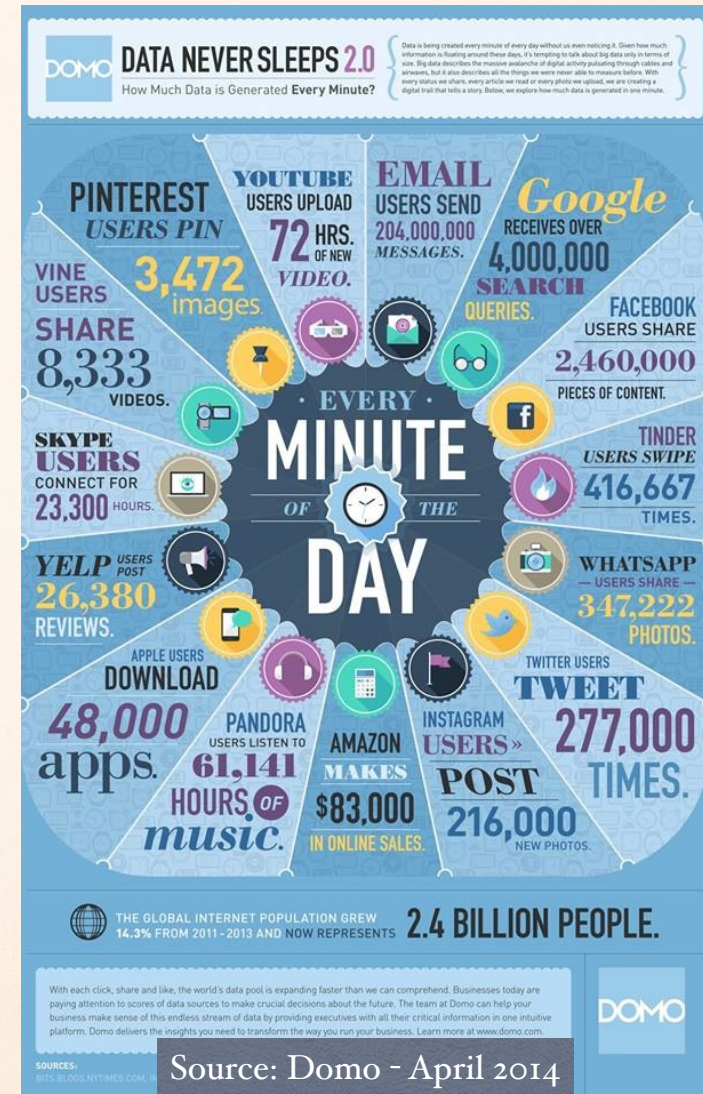
DEMOGRAPHICS

- *Global
 - *2.4 billion internet users (2012)
 - *5 billion mobile phone users
 - *1.5 billion smartphone users
 - *500+ million photos (daily)
 - *100 hours of YouTube video loaded (min)

Source: FedTech June 2013

NUMBERS

- *Every minute
- *61,000+ hours of music
- *277,000 Tweets
- *216,000 Instagram posts
- *4,000,000 Google Searches
- *2,460,000 Facebook shares

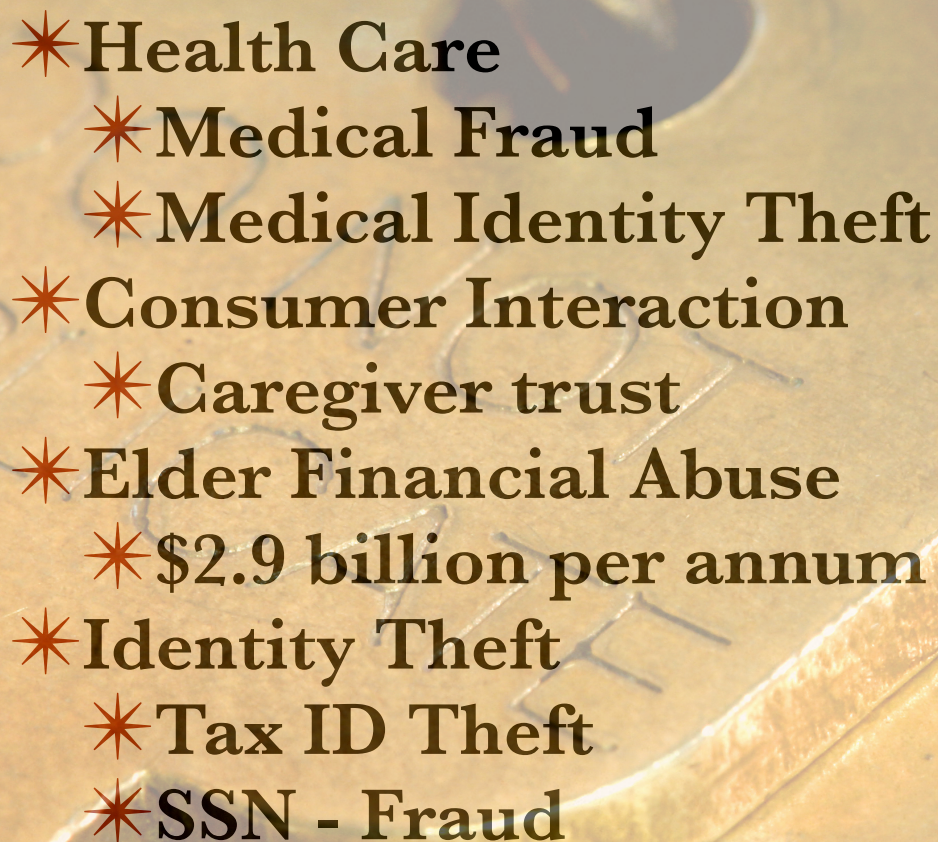


WHAT ARE WE DOING?

- * **Everything !**
- * **Social Security**
- * **Health**
- * **Taxes**
- * **Banking**
- * **Insurance**
- * **Shopping**
- * **Email**
- * **Social Engagement**



THREATS?

- 
- *Health Care
 - *Medical Fraud
 - *Medical Identity Theft
 - *Consumer Interaction
 - *Caregiver trust
 - *Elder Financial Abuse
 - *\$2.9 billion per annum
 - *Identity Theft
 - *Tax ID Theft
 - *SSN - Fraud

Your Device

- ◆ Operating system
- ◆ Security software
- ◆ Pins and passwords
- ◆ Authentication
- ◆ Location
- ◆ WiFi
- ◆ WiFi home network
- ◆ Applications
- ◆ Blue tooth
- ◆ Guest Accounts
- ◆ Travel with device

You

- ◆ Applications
- ◆ Single sign-on
- ◆ Privacy
- ◆ Email
- ◆ PHISH/SMISH
- ◆ Friending
- ◆ TMI
- ◆ Heartbleed

YOUR DEVICE

- ◆ Operating system
- ◆ Security software
- ◆ Pins and passwords
- ◆ Authentication
- ◆ Location
- ◆ WiFi
- ◆ WiFi home network
- ◆ Applications
- ◆ Blue tooth
- ◆ Guest Accounts
- ◆ Travel with device

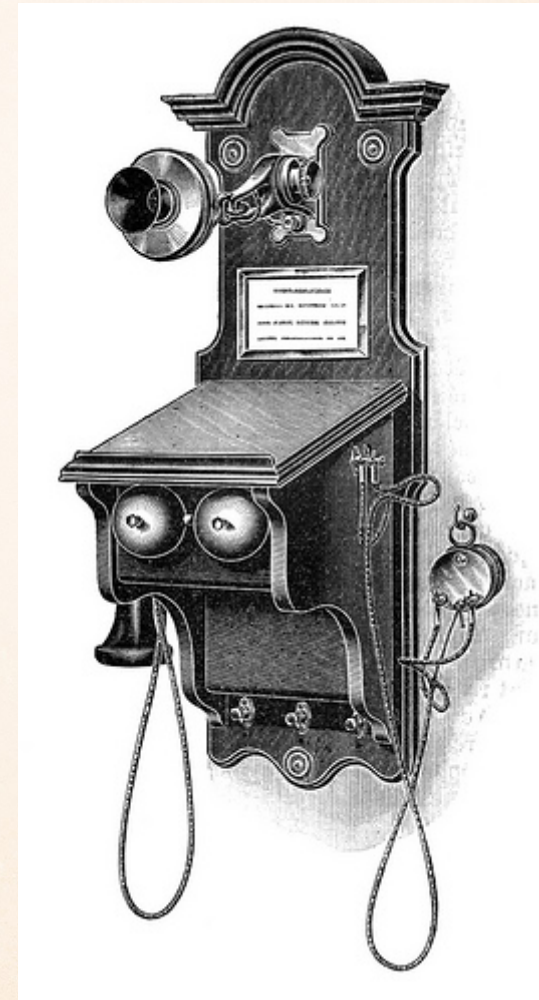
OPERATING SYSTEM

Updates

- ❖ Vulnerabilities

End of Life

- ❖ Windows XP?
- ❖ OS X Lion?



SECURITY SOFTWARE

Laptop/Desktop

- ❖ Virus Scan
- ❖ Firewall
- ❖ Malware/Crimeware

Mobile

- ❖ Malware
- ❖ Virus



PINS & PASSWORDS

❖ Passwords:

- ❖ Make them strong - s?9stATAS53E
- ❖ Do NOT reuse
- ❖ Use a password manager

❖ PINS

- ❖ All devices



AUTHENTICATION

- ❖ Single sign-on - understand the perils
- ❖ Facebook, Twitter, Google, etc - all have two-factor
- ❖ Two-Factor
- ❖ Bio-metric



LOCATION

All Devices

- ❖ GPS — on/off
- ❖ Sharing — on/off

Mobile

- ❖ Application specific?
 - ❖ Maps?
 - ❖ Location based Apps?
 - ❖ Retailer?
 - ❖ Social networks



WI-FI

Device

- ❖ No Auto-Connect

Behavior

- ❖ Discretion
- ❖ Browser: HTTPS
- ❖ Virtual Private Network



WI-FI HOME NETWORK

- ❖ Change Userid & Password
- ❖ WPA2 encryption
- ❖ MAC filtering
- ❖ Guest Network (if available)
- ❖ SSID



APPLICATIONS

Settings

- ❖ Access
- ❖ Sharing
- ❖ Check settings regularly



BLUE-TOOTH

Settings

- ❖ On/Off
- ❖ Searching
- ❖ Sharing
- ❖ Check settings regularly



GUEST ACCOUNTS

Three Good Reasons

- ❖ Unable to adjust device settings
- ❖ Full Control
- ❖ Files are temp



TRAVEL WITH A DEVICE?

Laptops & Drives

- ❖ Use cable locks
- ❖ Enable password access
- ❖ Securely store
- ❖ Enable remote locate software



YOU

- ◆ Applications
- ◆ Single sign-on
- ◆ Privacy
- ◆ Email
- ◆ PHISH/SMISH
- ◆ Friending
- ◆ TMI
- ◆ Heartbleed

APPLICATIONS

- ❖ Download from trusted sources
- ❖ Check settings
- ❖ Create alerts for apps which use your info
- ❖ Games - obfuscate locale & identity



PRIVACY

- ❖ Do you share information?
- ❖ Know who is doing what to your data
- ❖ Application settings
- ❖ Device sharing



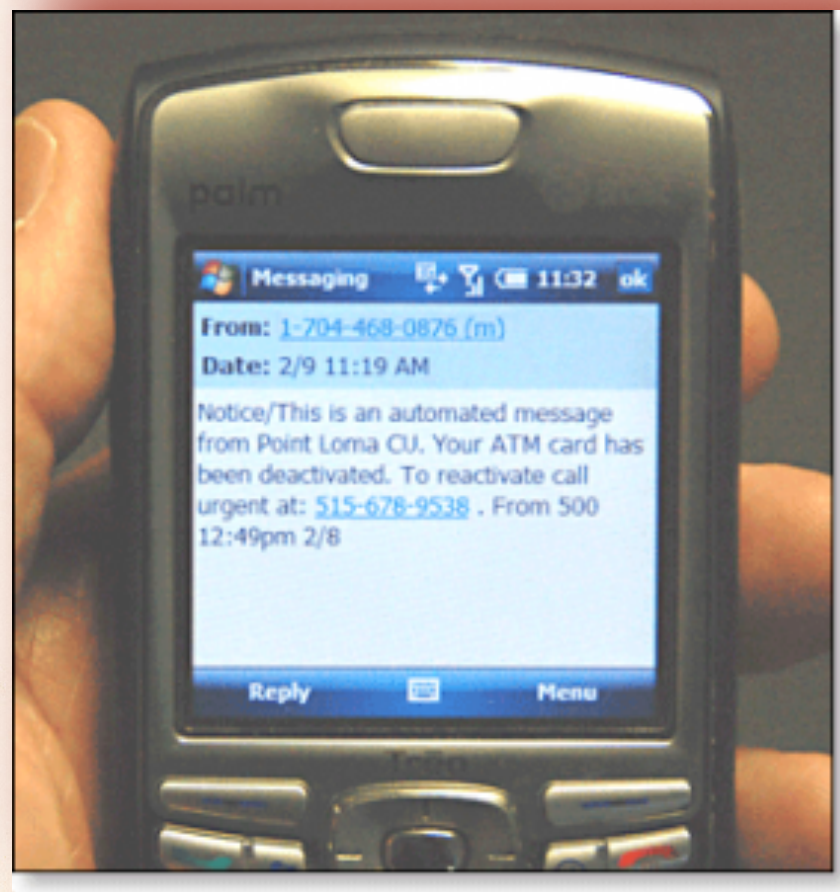
EMAIL

- ❖ Friend or Foe?
- ❖ Check headers if suspicious
- ❖ Clues:
 - ❖ “Look at this photo...”
 - ❖ “Look what they said...”



PHISH - SMISH

- ❖ Email
- ❖ Websites
- ❖ Social Networks
- ❖ SMS/Text



FRIENDING THE WORLD

- ❖ Have a personal policy of engagement.
- ❖ Friend's friends may not be your Friend
- ❖ Different profiles for different interests?



TMI

- ❖ Personal Identifying Information
- ❖ Protected Health Information
- ❖ Obscure knowledge based clues
- ❖ Social Networks
- ❖ Information harvesting
- ❖ Do NOT over share
- ❖ Identity Theft



HEARTBLEED

- ❖ What is it?
- ❖ What can you do?
- ❖ Password Change Required
- ❖ Be alert to Phish



Trend Micro Heartbleed Detector

By now you have probably heard about the Heartbleed bug, which criminals can use to capture data from websites protected by SSL (Secure Sockets Layer) encryption. This kind of website usually shows a "lock" symbol next to its address in your web browser.

To find out if a shopping, financial, or other secured website suffers from this problem, just provide its address below.

https://

Check Now



Good news, this site does not seem to have the HeartBleed vulnerability.

You can learn more about this vulnerability on the [Trend Micro Fearless Web blog](#).



RECAP

Online Safety

- * Device security is important
- * Keep software up-to-date
- * Do not overshare
- * You can keep yourself safe

Thank you!

Christopher Burgess
Prevendra, Inc.
PO Box 974
Woodinville, WA 98072
Info@Prevendra.com

 425-318-7860  [@BurgessCT](https://twitter.com/BurgessCT)
 [@SafetySeniors](https://twitter.com/SafetySeniors)

 **PREVENDRA**
Keeping You Safe & Secure