Security and Privacy and Anonymity (Oh My!)

Paranoia

"Strange how paranoia can link up with reality now and then."

Philip K. Dick
A Scanner Darkly

"Just because you're paranoid doesn't mean they aren't after you."

Joseph Heller
Catch 22

"Paranoia is just having the right information."

William S. Burroughs

Paranoia, but don't let the headlines cause you do do anything rash.

Some Definitions

- **Security**—is the degree of resistance to, or protection from, harm.
- **Privacy**—is the ability of an individual or group to seclude themselves or information about themselves and thereby express themselves selectively.
- **Anonymity**—the state of an individual's personal identity, or personally identifiable information, being publicly unknown.

Thursday, May 15, 14

Security - make sure the hardware works right and for you (not hijacked)

Privacy - what you do is your business, not anyone else's

Anonymity - useful for activists, reporters

Security

What is Security? (specifically Computer Security)

from Wikipedia

Confidentiality: Making sure people cannot acquire information they should not (keeping secrets)

Integrity: Making sure people cannot change information they should not (protecting data)

Availability: Making sure people cannot stop the computer from doing its job

What is Security? (specifically Computer Security)

"Computer security is a branch of information technology known as information security which is intended to protect computers. Computer security has three main goals:

from Wikipedia

Confidentiality: Making sure people cannot acquire information they should not (keeping secrets)

Integrity: Making sure people cannot change information they should not (protecting data)

Availability: Making sure people cannot stop the computer from doing its job

What is Security? (specifically Computer Security)

"Computer security is a branch of information technology known as information security which is intended to protect computers. Computer security has three main goals:

- Confidentiality

from Wikipedia

Confidentiality: Making sure people cannot acquire information they should not (keeping secrets)

Integrity: Making sure people cannot change information they should not (protecting data)

Availability: Making sure people cannot stop the computer from doing its job

What is Security? (specifically Computer Security)

"Computer security is a branch of information technology known as information security which is intended to protect computers. Computer security has three main goals:

- Confidentiality
- Integrity

from Wikipedia

Thursday, May 15, 14

Confidentiality: Making sure people cannot acquire information they should not (keeping secrets)

Integrity: Making sure people cannot change information they should not (protecting data)

Availability: Making sure people cannot stop the computer from doing its job

What is Security? (specifically Computer Security)

"Computer security is a branch of information technology known as information security which is intended to protect computers. Computer security has three main goals:

- Confidentiality
- Integrity
- Availability"

from Wikipedia

Confidentiality: Making sure people cannot acquire information they should not (keeping secrets)

Integrity: Making sure people cannot change information they should not (protecting data)

Availability: Making sure people cannot stop the computer from doing its job

How is Security related to Privacy?

How is Security related to Privacy?

- Privacy is one aspect of security but it emphasizes different goals

How is Security related to Privacy?

- Privacy is one aspect of security but it emphasizes different goals
- Security enhances the protection of privacy, but does not solve the the privacy protection problem

Wikipedia's list of basic security methods

(in approximate order of strength)

Wikipedia's list of basic security methods

(in approximate order of strength)

- Limit access to computers to "safe" users

Wikipedia's list of basic security methods

(in approximate order of strength)

- Limit access to computers to "safe" users
- Peripherals which block any "unsafe" activity

Wikipedia's list of basic security methods

(in approximate order of strength)

- Limit access to computers to "safe" users
- Peripherals which block any "unsafe" activity
- Firewall and antivirus software

US Government Computer Security Information Resources

OnGuardOnline.gov is the federal government’s website to help you be safe, secure and responsible online (DHS, Department of Commerce, Department of State, FCC)

US-CERT.gov, United States Computer Emergency Readiness Team (DHS)
US-CERT is the 24-hour operational arm of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC)

US Government Computer Security Information Resources

- OnGuardOnline.gov
  http://www.onguardonline.gov

OnGuardOnline.gov is the federal government's website to help you be safe, secure and responsible online (DHS, Department of Commerce, Department of State, FCC)

US-CERT.gov, United States Computer Emergency Readiness Team (DHS)
US-CERT is the 24-hour operational arm of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC)

US Government Computer Security Information Resources

- OnGuardOnline.gov
  http://www.onguardonline.gov

- US-CERT.gov
  https://www.us-cert.gov
  https://www.us-cert.gov/cas/tips/

OnGuardOnline.gov is the federal government's website to help you be safe, secure and responsible online (DHS, Department of Commerce, Department of State, FCC)

US-CERT.gov, United States Computer Emergency Readiness Team (DHS)
US-CERT is the 24-hour operational arm of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC)

OnGuardOnline.gov Recommendations

Use Security Software That Updates Automatically
Most security software can update automatically; set yours to do so. Also, set your operating system and web browser to update automatically.
Don’t buy security software in response to unexpected pop-up messages or emails, especially messages that claim to have scanned your computer and found malware. Scammers send messages like these to try to get you to buy worthless software, or worse, to “break and enter” your computer.

** MacTracker is BAD!

Treat Your Personal Information Like Cash
Don’t hand it out to just anyone. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. So every time you are asked for your personal information – whether in a web form, an email, a text, or a phone message – think about whether you can really trust the request. In an effort to steal your information, scammers will do everything they can to appear trustworthy. Learn more about scammers who phish for your personal information.

Check Out Companies to Find out Who You’re Really Dealing With
When you’re online, a little research can save you a lot of money. If you see an ad or an offer that looks good to you, take a moment to check out the company behind it. Type the company or product name into your favorite search engine with terms like “review,” “complaint,” or “scam.” If you find bad reviews, you’ll have to decide if the offer is worth the risk. If you can’t find contact information for the company, take your business elsewhere.
Don’t assume that an ad you see on a reputable site is trustworthy. The fact that a site features an ad for another site doesn’t mean that it endorses the advertised site, or is even familiar with it.

OnGuardOnline.gov Recommendations

- Use security software that updates automatically

Use Security Software That Updates Automatically
Most security software can update automatically; set yours to do so. Also, set your operating system and web browser to update automatically.
Don’t buy security software in response to unexpected pop-up messages or emails, especially messages that claim to have scanned your computer and found malware. Scammers send messages like these to try to get you to buy worthless software, or worse, to “break and enter” your computer.

** MacTracker is BAD!

Treat Your Personal Information Like Cash
Don’t hand it out to just anyone. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. So every time you are asked for your personal information – whether in a web form, an email, a text, or a phone message – think about whether you can really trust the request. In an effort to steal your information, scammers will do everything they can to appear trustworthy. Learn more about scammers who phish for your personal information.

Check Out Companies to Find out Who You’re Really Dealing With
When you’re online, a little research can save you a lot of money. If you see an ad or an offer that looks good to you, take a moment to check out the company behind it. Type the company or product name into your favorite search engine with terms like “review,” “complaint,” or “scam.” If you find bad reviews, you’ll have to decide if the offer is worth the risk. If you can’t find contact information for the company, take your business elsewhere.
Don’t assume that an ad you see on a reputable site is trustworthy. The fact that a site features an ad for another site doesn’t mean that it endorses the advertised site, or is even familiar with it.

OnGuardOnline.gov Recommendations

- Use security software that updates automatically
- Treat your personal information like cash

Use Security Software That Updates Automatically
Most security software can update automatically; set yours to do so. Also, set your operating system and web browser to update automatically.

Don’t buy security software in response to unexpected pop-up messages or emails, especially messages that claim to have scanned your computer and found malware. Scammers send messages like these to try to get you to buy worthless software, or worse, to “break and enter” your computer.

** MacTracker is BAD!

Treat Your Personal Information Like Cash
Don’t hand it out to just anyone. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. So every time you are asked for your personal information – whether in a web form, an email, a text, or a phone message – think about whether you can really trust the request. In an effort to steal your information, scammers will do everything they can to appear trustworthy. Learn more about scammers who phish for your personal information.

Check Out Companies to Find out Who You’re Really Dealing With
When you’re online, a little research can save you a lot of money. If you see an ad or an offer that looks good to you, take a moment to check out the company behind it. Type the company or product name into your favorite search engine with terms like “review,” “complaint,” or “scam.” If you find bad reviews, you’ll have to decide if the offer is worth the risk. If you can’t find contact information for the company, take your business elsewhere.
Don’t assume that an ad you see on a reputable site is trustworthy. The fact that a site features an ad for another site doesn’t mean that it endorses the advertised site, or is even familiar with it.

OnGuardOnline.gov Recommendations

- Use security software that updates automatically
- Treat your personal information like cash
- Check out companies to find out who you're really dealing with

Thursday, May 15, 14

Use Security Software That Updates Automatically
Most security software can update automatically; set yours to do so. Also, set your operating system and web browser to update automatically.

Don't buy security software in response to unexpected pop-up messages or emails, especially messages that claim to have scanned your computer and found malware. Scammers send messages like these to try to get you to buy worthless software, or worse, to "break and enter" your computer.

** MacTracker is BAD!

Treat Your Personal Information Like Cash
Don't hand it out to just anyone. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. So every time you are asked for your personal information – whether in a web form, an email, a text, or a phone message – think about whether you can really trust the request. In an effort to steal your information, scammers will do everything they can to appear trustworthy. Learn more about scammers who phish for your personal information.

Check Out Companies to Find out Who You're Really Dealing With
When you're online, a little research can save you a lot of money. If you see an ad or an offer that looks good to you, take a moment to check out the company behind it. Type the company or product name into your favorite search engine with terms like "review," "complaint," or "scam." If you find bad reviews, you'll have to decide if the offer is worth the risk. If you can't find contact information for the company, take your business elsewhere.
Don't assume that an ad you see on a reputable site is trustworthy. The fact that a site features an ad for another site doesn't mean that it endorses the advertised site, or is even familiar with it.

OnGuardOnline.gov Recommendations (cont'd)

Give Personal Information Over Encrypted Websites Only

If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for https at the beginning of the web address (the "s" is for secure).

Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, the entire account could be vulnerable. Look for https on every page of the site you're on, not just where you sign in.

Protect Your Passwords

Back Up Your Files

No system is completely secure. Copy important files onto a removable disc or an external hard drive, and store it in a safe place. If your computer is compromised, you'll still have access to your files.

OnGuardOnline.gov Recommendations (cont'd)

- Give personal information over encrypted websites only

Give Personal Information Over Encrypted Websites Only

If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for https at the beginning of the web address (the "s" is for secure).

Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, the entire account could be vulnerable. Look for https on every page of the site you're on, not just where you sign in.

Protect Your Passwords

Back Up Your Files

No system is completely secure. Copy important files onto a removable disc or an external hard drive, and store it in a safe place. If your computer is compromised, you'll still have access to your files.

OnGuardOnline.gov Recommendations (cont'd)

- Give personal information over encrypted websites only
- Protect your passwords

Thursday, May 15, 14

Give Personal Information Over Encrypted Websites Only
If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for https at the beginning of the web address (the "s" is for secure).
Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, the entire account could be vulnerable. Look for https on every page of the site you're on, not just where you sign in.

Protect Your Passwords

Back Up Your Files
No system is completely secure. Copy important files onto a removable disc or an external hard drive, and store it in a safe place. If your computer is compromised, you'll still have access to your files.

OnGuardOnline.gov Recommendations (cont'd)

- Give personal information over encrypted websites only
- Protect your passwords
- Back up your files

Thursday, May 15, 14

Give Personal Information Over Encrypted Websites Only
If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for https at the beginning of the web address (the "s" is for secure).
Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, the entire account could be vulnerable. Look for https on every page of the site you're on, not just where you sign in.

Protect Your Passwords

Back Up Your Files
No system is completely secure. Copy important files onto a removable disc or an external hard drive, and store it in a safe place. If your computer is compromised, you'll still have access to your files.

US-CERT.gov Recommendations

Lock your computer when you are away from it. Even if you only step away from your computer for a few minutes, it's enough time for someone else to destroy or corrupt your information. Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information.

Disconnect your computer from the Internet when you aren't using it. The development of technologies such as DSL and cable modems have made it possible for users to be online all the time, but this convenience comes with risks. The likelihood that attackers or viruses scanning the network for available computers will target your computer becomes much higher if your computer is always connected. Depending on what method you use to connect to the Internet, disconnecting may mean disabling a wireless connection, turning off your computer or modem, or disconnecting cables. When you are connected, make sure that you have a firewall enabled (see Understanding Firewalls for more information).

Evaluate your security settings. Most software, including browsers and email programs, offers a variety of features that you can tailor to meet your needs and requirements. Enabling certain features to increase convenience or functionality may leave you more vulnerable to being attacked. It is important to examine the settings, particularly the security settings, and select options that meet your needs without putting you at increased risk. If you install a patch or a new version of the software, or if you hear of something that might affect your settings, reevaluate your settings to make sure they are still appropriate (see Understanding Patches, Safeguarding Your Data, and Evaluating Your Web Browser's Security Settings for more information).

US-CERT.gov Recommendations

- Lock your computer when you are away from it

Thursday, May 15, 14

Lock your computer when you are away from it. Even if you only step away from your computer for a few minutes, it's enough time for someone else to destroy or corrupt your information. Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information.

Disconnect your computer from the Internet when you aren't using it. The development of technologies such as DSL and cable modems have made it possible for users to be online all the time, but this convenience comes with risks. The likelihood that attackers or viruses scanning the network for available computers will target your computer becomes much higher if your computer is always connected. Depending on what method you use to connect to the Internet, disconnecting may mean disabling a wireless connection, turning off your computer or modem, or disconnecting cables. When you are connected, make sure that you have a firewall enabled (see Understanding Firewalls for more information).

Evaluate your security settings. Most software, including browsers and email programs, offers a variety of features that you can tailor to meet your needs and requirements. Enabling certain features to increase convenience or functionality may leave you more vulnerable to being attacked. It is important to examine the settings, particularly the security settings, and select options that meet your needs without putting you at increased risk. If you install a patch or a new version of the software, or if you hear of something that might affect your settings, reevaluate your settings to make sure they are still appropriate (see Understanding Patches, Safeguarding Your Data, and Evaluating Your Web Browser's Security Settings for more information).

US-CERT.gov Recommendations

- Lock your computer when you are away from it
- Disconnect your computer from the Internet when you aren't using it

Lock your computer when you are away from it. Even if you only step away from your computer for a few minutes, it's enough time for someone else to destroy or corrupt your information. Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information.

Disconnect your computer from the Internet when you aren't using it. The development of technologies such as DSL and cable modems have made it possible for users to be online all the time, but this convenience comes with risks. The likelihood that attackers or viruses scanning the network for available computers will target your computer becomes much higher if your computer is always connected. Depending on what method you use to connect to the Internet, disconnecting may mean disabling a wireless connection, turning off your computer or modem, or disconnecting cables. When you are connected, make sure that you have a firewall enabled (see Understanding Firewalls for more information).

Evaluate your security settings. Most software, including browsers and email programs, offers a variety of features that you can tailor to meet your needs and requirements. Enabling certain features to increase convenience or functionality may leave you more vulnerable to being attacked. It is important to examine the settings, particularly the security settings, and select options that meet your needs without putting you at increased risk. If you install a patch or a new version of the software, or if you hear of something that might affect your settings, reevaluate your settings to make sure they are still appropriate (see Understanding Patches, Safeguarding Your Data, and Evaluating Your Web Browser's Security Settings for more information).

US-CERT.gov Recommendations

- Lock your computer when you are away from it
- Disconnect your computer from the Internet when you aren't using it
- Evaluate your security settings

Lock your computer when you are away from it. Even if you only step away from your computer for a few minutes, it's enough time for someone else to destroy or corrupt your information. Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information.

Disconnect your computer from the Internet when you aren't using it. The development of technologies such as DSL and cable modems have made it possible for users to be online all the time, but this convenience comes with risks. The likelihood that attackers or viruses scanning the network for available computers will target your computer becomes much higher if your computer is always connected. Depending on what method you use to connect to the Internet, disconnecting may mean disabling a wireless connection, turning off your computer or modem, or disconnecting cables. When you are connected, make sure that you have a firewall enabled (see Understanding Firewalls for more information).

Evaluate your security settings. Most software, including browsers and email programs, offers a variety of features that you can tailor to meet your needs and requirements. Enabling certain features to increase convenience or functionality may leave you more vulnerable to being attacked. It is important to examine the settings, particularly the security settings, and select options that meet your needs without putting you at increased risk. If you install a patch or a new version of the software, or if you hear of something that might affect your settings, reevaluate your settings to make sure they are still appropriate (see Understanding Patches, Safeguarding Your Data, and Evaluating Your Web Browser's Security Settings for more information).

US-CERT.gov Recommendations (cont'd)

Protect your computer against power surges and brief outages. Aside from providing outlets to plug in your computer and all of its peripherals, some power strips protect your computer against power surges. Many power strips now advertise compensation if they do not effectively protect your computer. Power strips alone will not protect you from power outages, but there are products that do offer an uninterruptible power supply when there are power surges or outages. During a lightning storm or construction work that increases the odds of power surges, consider shutting your computer down and unplugging it from all power sources.

Back up all of your data. Whether or not you take steps to protect yourself, there will always be a possibility that something will happen to destroy your data. You have probably already experienced this at least once— losing one or more files due to an accident, a virus or worm, a natural event, or a problem with your equipment. Regularly backing up your data on a CD or network reduces the stress and other negative consequences that result from losing important information (see Real-World Warnings Keep You Safe Online for more information). Determining how often to back up your data is a personal decision. If you are constantly adding or changing data, you may find weekly backups to be the best alternative; if your content rarely changes, you may decide that your backups do not need to be as frequent. You don't need to back up software that you own on CD-ROM or DVD-ROM—you can reinstall the software from the original media if necessary.

US-CERT.gov Recommendations (cont'd)

- Protect your computer against power surges and brief outages

Protect your computer against power surges and brief outages. Aside from providing outlets to plug in your computer and all of its peripherals, some power strips protect your computer against power surges. Many power strips now advertise compensation if they do not effectively protect your computer. Power strips alone will not protect you from power outages, but there are products that do offer an uninterruptible power supply when there are power surges or outages. During a lightning storm or construction work that increases the odds of power surges, consider shutting your computer down and unplugging it from all power sources.

Back up all of your data. Whether or not you take steps to protect yourself, there will always be a possibility that something will happen to destroy your data. You have probably already experienced this at least once— losing one or more files due to an accident, a virus or worm, a natural event, or a problem with your equipment. Regularly backing up your data on a CD or network reduces the stress and other negative consequences that result from losing important information (see Real-World Warnings Keep You Safe Online for more information). Determining how often to back up your data is a personal decision. If you are constantly adding or changing data, you may find weekly backups to be the best alternative; if your content rarely changes, you may decide that your backups do not need to be as frequent. You don't need to back up software that you own on CD-ROM or DVD-ROM—you can reinstall the software from the original media if necessary.

US-CERT.gov Recommendations (cont'd)

- Protect your computer against power surges and brief outages
- Back up all of your data

Thursday, May 15, 14

Protect your computer against power surges and brief outages. Aside from providing outlets to plug in your computer and all of its peripherals, some power strips protect your computer against power surges. Many power strips now advertise compensation if they do not effectively protect your computer. Power strips alone will not protect you from power outages, but there are products that do offer an uninterruptible power supply when there are power surges or outages. During a lightning storm or construction work that increases the odds of power surges, consider shutting your computer down and unplugging it from all power sources.

Back up all of your data. Whether or not you take steps to protect yourself, there will always be a possibility that something will happen to destroy your data. You have probably already experienced this at least once— losing one or more files due to an accident, a virus or worm, a natural event, or a problem with your equipment. Regularly backing up your data on a CD or network reduces the stress and other negative consequences that result from losing important information (see Real-World Warnings Keep You Safe Online for more information). Determining how often to back up your data is a personal decision. If you are constantly adding or changing data, you may find weekly backups to be the best alternative; if your content rarely changes, you may decide that your backups do not need to be as frequent. You don't need to back up software that you own on CD-ROM or DVD-ROM—you can reinstall the software from the original media if necessary.

Passwords

25 Most Popular Passwords of 2012 (according to SplashData)

Most popular passwords

25 Most Popular Passwords of 2012 (according to SplashData)

- password

Most popular passwords

25 Most Popular Passwords of 2012 (according to SplashData)

- password
- 123456
- 12345678
- abc123
- qwerty
- monkey
- letmein

Most popular passwords

25 Most Popular Passwords of 2012 (according to SplashData)

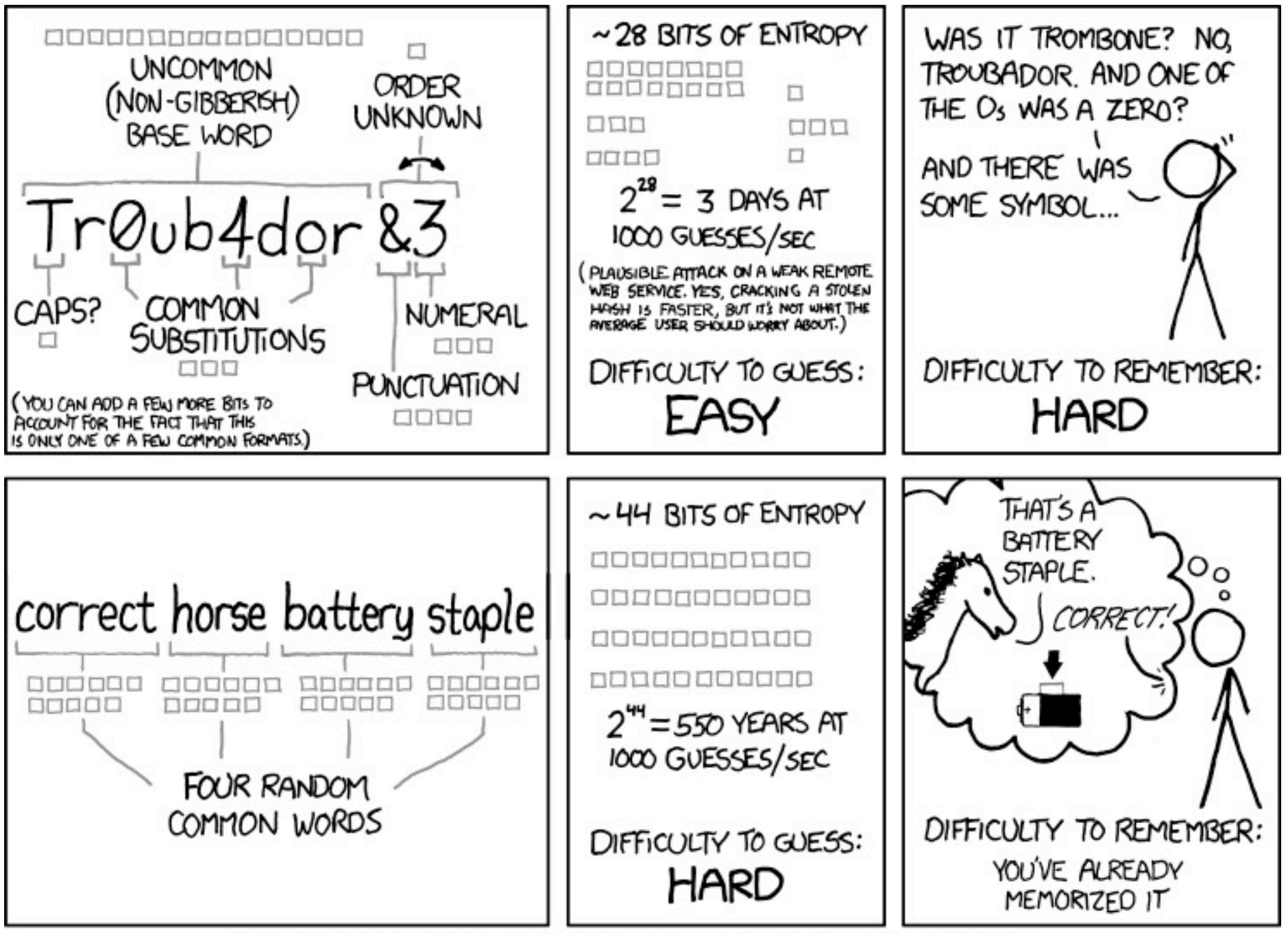
- password
- 123456
- 12345678
- abc123
- qwerty
- monkey
- letmein
- dragon
- 111111
- baseball
- iloveyou
- trustno l
- 1234567
- sunshine

Most popular passwords

25 Most Popular Passwords of 2012 (according to SplashData)

- password
- 123456
- 12345678
- abc123
- qwerty
- monkey
- letmein
- dragon
- 111111
- baseball
- iloveyou
- trustno1
- 1234567
- sunshine
- master
- 123123
- welcome
- shadow
- ashley
- football
- jesus
- michael
- ninja
- mustang
- password1

Most popular passwords



from xkcd.com

Since the appearance of this cartoon, “correct horse battery staple” is in hackers’ password lists

OnGuardOnline.gov Password Recommendations

The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.

Mix letters, numbers, and special characters. Try to be unpredictable – don’t use your name, birthdate, or common words.

Don’t use the same password for many accounts. If it’s stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts.

OnGuardOnline.gov Password Recommendations

- The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.

Thursday, May 15, 14

The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.

Mix letters, numbers, and special characters. Try to be unpredictable – don’t use your name, birthdate, or common words.

Don’t use the same password for many accounts. If it’s stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts.

OnGuardOnline.gov Password Recommendations

- The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.
- Mix letters, numbers, and special characters. Try to be unpredictable – don't use your name, birthdate, or common words.

Thursday, May 15, 14

The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.

Mix letters, numbers, and special characters. Try to be unpredictable – don't use your name, birthdate, or common words.

Don't use the same password for many accounts. If it's stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts.

OnGuardOnline.gov Password Recommendations

- The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.
- Mix letters, numbers, and special characters. Try to be unpredictable – don't use your name, birthdate, or common words.
- Don't use the same password for many accounts.

Thursday, May 15, 14

The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.

Mix letters, numbers, and special characters. Try to be unpredictable – don't use your name, birthdate, or common words.

Don't use the same password for many accounts. If it's stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts.

OnGuardOnline.gov Password Recommendations

Don’t share passwords on the phone, in texts or by email. Legitimate companies will not send you messages asking for your password. If you get such a message, it’s probably a scam.

Keep your passwords in a secure place, out of plain sight.

OnGuardOnline.gov Password Recommendations

- Don’t share passwords on the phone, in texts or by email.

Thursday, May 15, 14

Don’t share passwords on the phone, in texts or by email. Legitimate companies will not send you messages asking for your password. If you get such a message, it’s probably a scam.

Keep your passwords in a secure place, out of plain sight.

OnGuardOnline.gov Password Recommendations

- Don’t share passwords on the phone, in texts or by email.
- Keep your passwords in a secure place, out of plain sight.

Thursday, May 15, 14

Don’t share passwords on the phone, in texts or by email. Legitimate companies will not send you messages asking for your password. If you get such a message, it’s probably a scam.

Keep your passwords in a secure place, out of plain sight.

US-CERT.gov Password Recommendations

US-CERT.gov Password Recommendations

- Don't use passwords that are based on personal information that can be easily accessed or guessed.

US-CERT.gov Password Recommendations

- Don't use passwords that are based on personal information that can be easily accessed or guessed.
- Don't use words that can be found in any dictionary of any language.

US-CERT.gov Password Recommendations

- Don't use passwords that are based on personal information that can be easily accessed or guessed.
- Don't use words that can be found in any dictionary of any language.
- Develop a mnemonic for remembering complex passwords.

US-CERT.gov Password Recommendations

US-CERT.gov Password Recommendations

- Use both lowercase and capital letters.

US-CERT.gov Password Recommendations

- Use both lowercase and capital letters.
- Use a combination of letters, numbers, and special characters.

US-CERT.gov Password Recommendations

- Use both lowercase and capital letters.
- Use a combination of letters, numbers, and special characters.
- Use passphrases when you can.

US-CERT.gov Password Recommendations

- Use both lowercase and capital letters.
- Use a combination of letters, numbers, and special characters.
- Use passphrases when you can.
- Use different passwords on different systems.

Firewalls

"A system designed to prevent unauthorized access to or from a private network. ... All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria."

from Webopedia
http://www.webopedia.com/TERM/F/firewall.html

Firewalls

Firewalls

- Hardware Firewalls

Firewalls

- Hardware Firewalls
- Software Firewalls

Hardwire Firewalls

Hardwire Firewalls

- In a home network, typically in the router

Hardwire Firewalls

- In a home network, typically in the router
- Apple's Airport Extreme has a firewall automatically enabled

Hardwire Firewalls

- In a home network, typically in the router
- Apple's Airport Extreme has a firewall automatically enabled
- Configuration of firewalls can be complex and requires "geek" level knowledge

Software Firewalls

Software Firewalls

- OS X has a built-in software firewall

Software Firewalls

- OS X has a built-in software firewall
- The OS X firewall is off by default

Software Firewalls

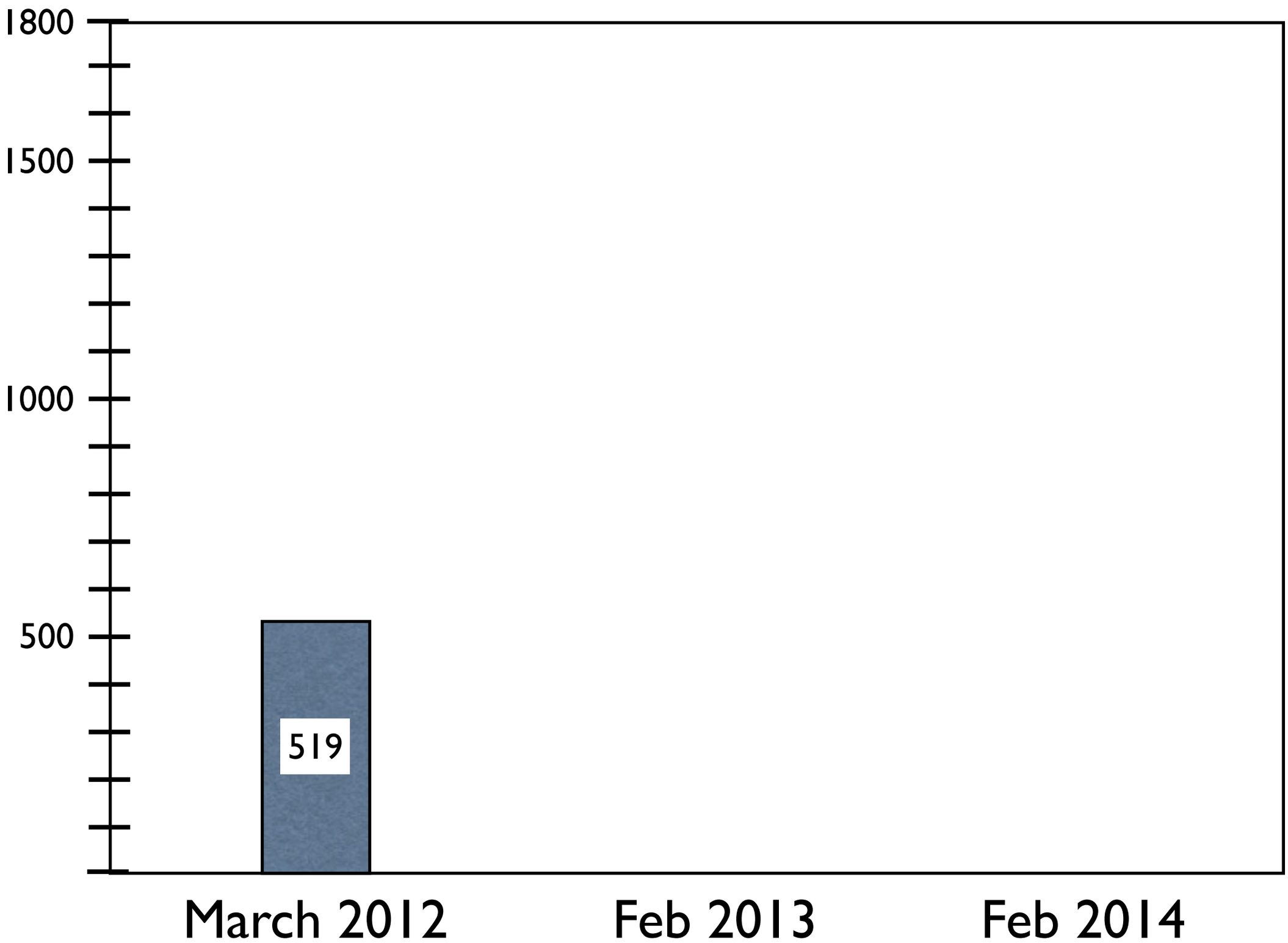
- OS X has a built-in software firewall
- The OS X firewall is off by default
- The OS X firewall is accessed via the Security & Privacy preferences panel (used to be Network)

Privacy

Difference between privacy and anonymity

- When you visit the doctor, that is **private** (ideally) but it is not anonymous: the doctor inspects your person and your history with great detail.
- If you go to Starbucks and buy a latte using cash, that's **anonymous** (since there's nothing linking you to the currency you use) but it's not private (since you're in a cafe with other people)

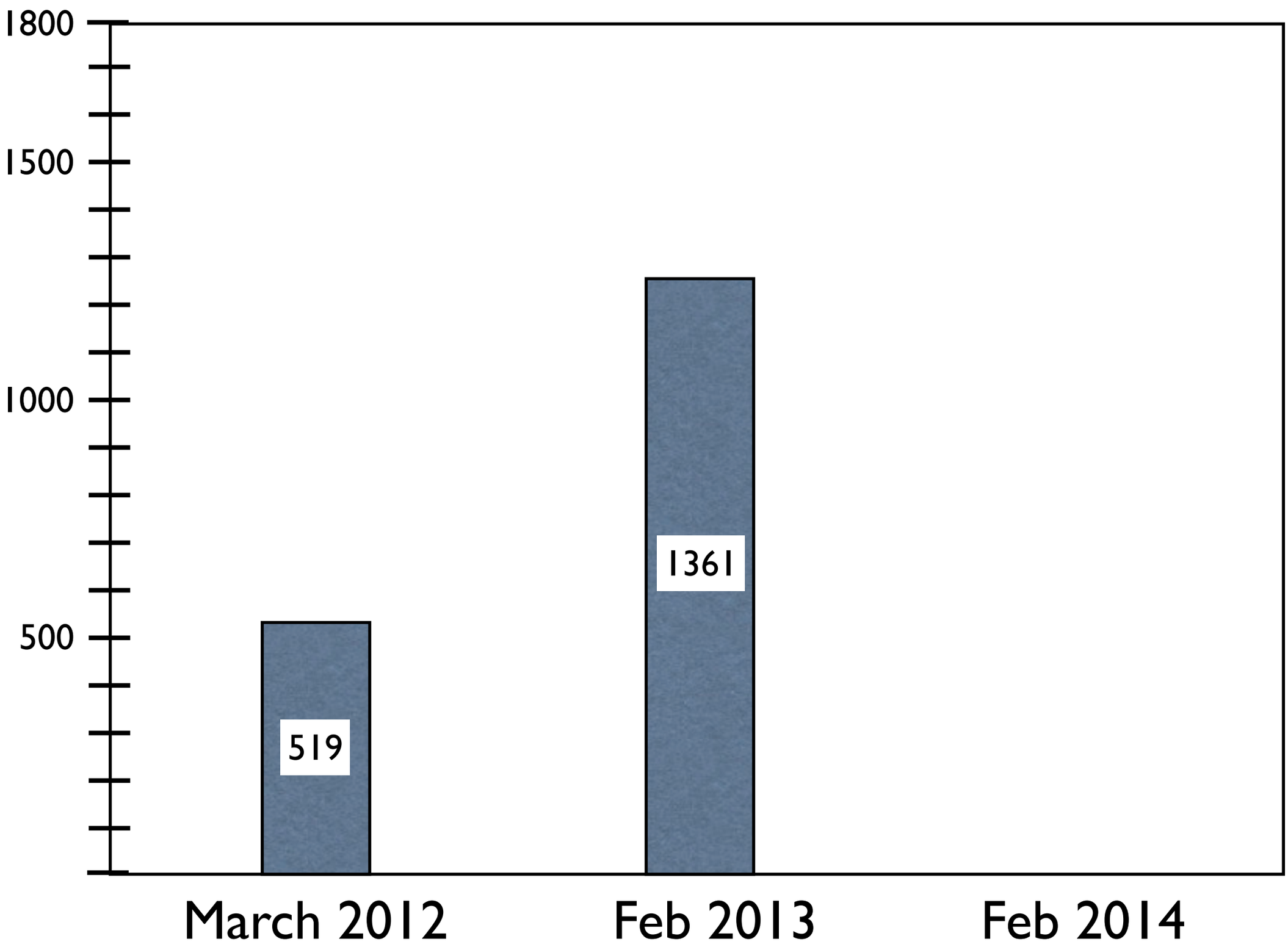
Who's Tracking You?



519 companies (March 2012)

As of Feb 18, 2013: total 1361 (162% increase)
Advertising: 661
Analytics: 251
Beacons: 282
Privacy: 18
Widgets: 149

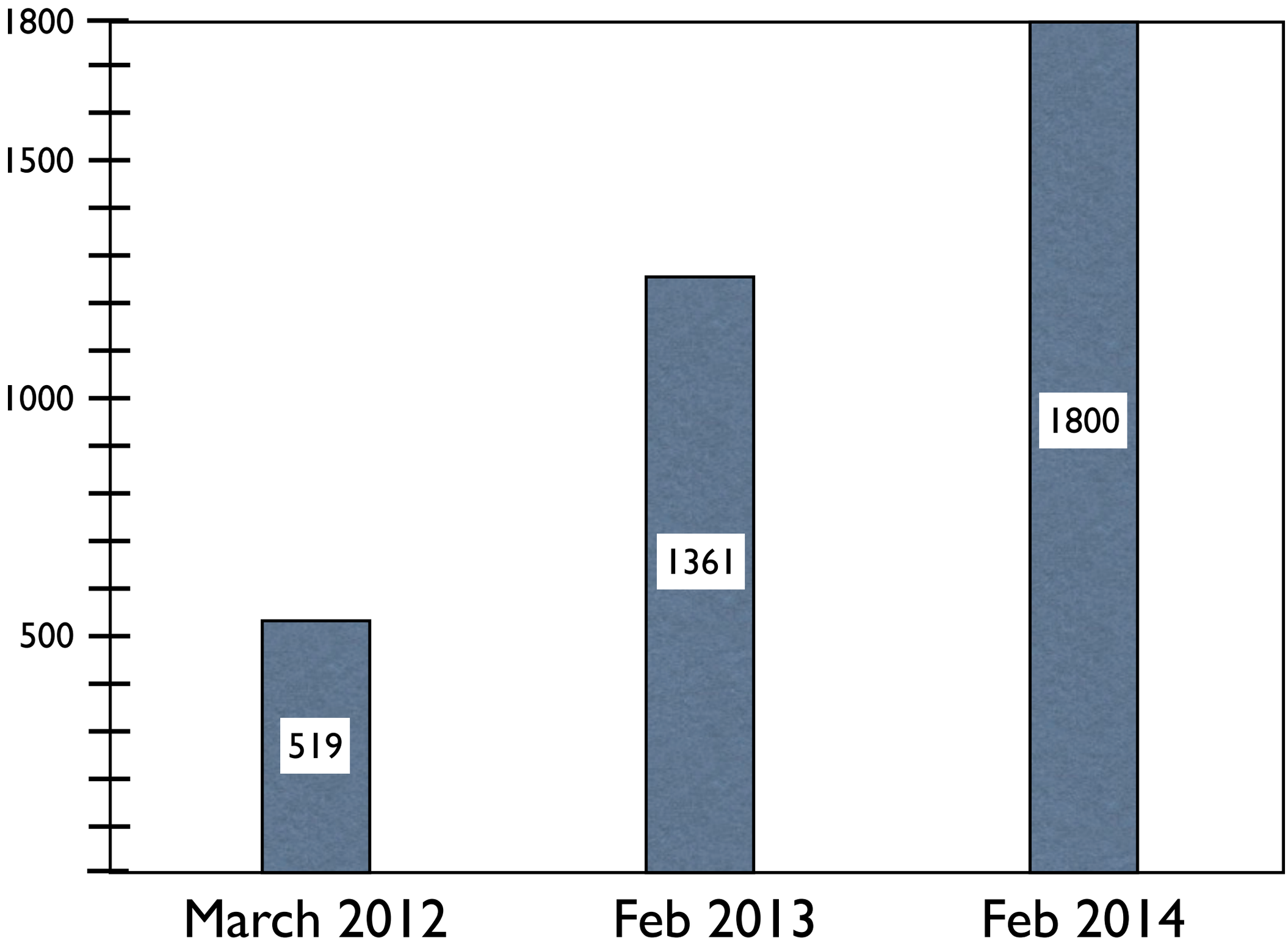
As of Feb 9, 2014: total 1800 (246% over 2 years, 32% over 1 year)
Advertising: 900
Analytics: 300
Beacons: 366
Privacy: 17
Widgets: 261



519 companies (March 2012)

As of Feb 18, 2013: total 1361 (162% increase)
Advertising: 661
Analytics: 251
Beacons: 282
Privacy: 18
Widgets: 149

As of Feb 9, 2014: total 1800 (246% over 2 years, 32% over 1 year)
Advertising: 900
Analytics: 300
Beacons: 366
Privacy: 17
Widgets: 261



519 companies (March 2012)

As of Feb 18, 2013: total 1361 (162% increase)
Advertising: 661
Analytics: 251
Beacons: 282
Privacy: 18
Widgets: 149

As of Feb 9, 2014: total 1800 (246% over 2 years, 32% over 1 year)
Advertising: 900
Analytics: 300
Beacons: 366
Privacy: 17
Widgets: 261

Why does it matter?

"If you are doing something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."

Eric Schmidt, CEO Google—2009

"You have zero privacy anyway.
Get over it."

Scott McNealy, CEO Sun Microsystems—12/20/99

Web Browsing

Simple Steps

- Private Browsing?

- Monitor “Flash Cookies”

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

private browsing only protects privacy against someone who has physical or remote access to you computer

Flash cookies are also referred to as “zombie” cookies

Security expert Charlie Miller “[The safest browser is] Chrome with no Flash installed. The main thing is not to install Flash!”

- Adjust browser settings
- Check and delete cookies
- Opt-out of Flash cookies

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager03.html

Advanced Steps

Opt-out

- The Network Advertising Initiative
  http://networkadvertising.org
- PrivacyChoice LLC
  http://privacychoice.org/choose

Privacy Plug-ins

- **Ghostery** (Safari, Firefox, Chrome)
  http://www.ghostery.com
- **Disconnect** (Safari, Firefox, Chrome, Opera)
  https://disconnect.me
- Abine **DoNotTrackMe** (Safari, Firefox, Chrome)
  https://www.abine.com
- **AdblockPlus** (Safari—beta, Firefox, Chrome, Opera, Android, Internet Explorer)
  https://adblockplus.org

The Heartbleed Bug 

Heartbleed comes from Hearbeat, the feature installed about 3 years ago

The Heartbleed Bug 

- Heartbleed is a server bug, not a user computer bug (http://heartbleed.com)

Heartbleed comes from Hearbeat, the feature installed about 3 years ago

The Heartbleed Bug 

- Heartbleed is a server bug, not a user computer bug (http://heartbleed.com)
- You should change your passwords if the server has fixed the bug (lastpass.com/heartbleed/ or https://filippo.io/Heartbleed/)

Heartbleed comes from Hearbeat, the feature installed about 3 years ago

The Heartbleed Bug 

- Heartbleed is a server bug, not a user computer bug (http://heartbleed.com)
- You should change your passwords if the server has fixed the bug (lastpass.com/heartbleed/ or https://filippo.io/Heartbleed/)
- xkcd cartoon explaining Heartbleed

Heartbleed comes from Hearbeat, the feature installed about 3 years ago

Web Browsing in Safari

Web Browsing in Safari

- Turn off 'Open "safe" files after downloading (Safari Preferences, General tab)

Web Browsing in Safari

- Turn off 'Open "safe" files after downloading (Safari Preferences, General tab)
- Disable Java in Preferences (Safari Preferences, Security tab, uncheck Enable Java)

Web Browsing (General)

Web Browsing (General)

- Use https whenever possible

Web Browsing (General)

- Use https whenever possible
- Use ONLY https when providing user information

Web Browsing (General)

- Use https whenever possible
- Use ONLY https when providing user information
- Never click a link from an unknown source (in an email, a web site or any other document)

Wi-Fi Hotspots

Wi-Fi Hotspots

- Most Wi-Fi hotspots are not encrypted and not secure (and some are set up just to capture your data)

Wi-Fi Hotspots

- Most Wi-Fi hotspots are not encrypted and not secure (and some are set up just to capture your data)
- Hacking tools are readily available (for example, Firesheep)

Wi-Fi Hotspots

Wi-Fi Hotspots

- Only send personal information to encrypted websites (look for “s” in https)

Wi-Fi Hotspots

- Only send personal information to encrypted websites (look for “s” in https)
- Logout when done

Wi-Fi Hotspots

- Only send personal information to encrypted websites (look for “s” in https)
- Logout when done
- Install Browser plug-ins (Firefox only)
  HTTPS Everywhere - https://www.eff.org/https-everywhere (Chrome & opera in beta)
  Force-TLS - http://forcetls.sidstamm.com/

Wi-Fi Hotspots

- Only send personal information to encrypted websites (look for "s" in https)
- Logout when done
- Install Browser plug-ins (Firefox only)
  HTTPS Everywhere - https://www.eff.org/https-everywhere (Chrome & opera in beta)
  Force-TLS - http://forcetls.sidstamm.com/
- Use a Virtual Private Network (VPN)

Wi-Fi Hotspots

Use a travel router to connect to a Wi-Fi hotspot or facility’s broadband.

will create a private, secure, wireless network with a robust firewall

Wi-Fi Hotspots

- If you travel, consider a travel router

Use a travel router to connect to a Wi-Fi hotspot or facility's broadband.

will create a private, secure, wireless network with a robust firewall

Wi-Fi Hotspots

- If you travel, consider a travel router
- 6 new travel routers reviewed

Use a travel router to connect to a Wi-Fi hotspot or facility's broadband.

will create a private, secure, wireless network with a robust firewall

Wi-Fi Hotspots

- If you travel, consider a travel router
- 6 new travel routers reviewed
- http://www.macworld.com/article/2153143/tested-6-new-travel-routers-that-can-deploy-a-secure-wi-fi-network-almost-anywhere.html#tk.rss_all

Use a travel router to connect to a Wi-Fi hotspot or facility's broadband.

will create a private, secure, wireless network with a robust firewall

Wi-Fi Hotspots

- If you travel, consider a travel router
- 6 new travel routers reviewed
- http://www.macworld.com/article/2153143/tested-6-new-travel-routers-that-can-deploy-a-secure-wi-fi-network-almost-anywhere.html#tk.rss_all
- $35-$100

Thursday, May 15, 14

Use a travel router to connect to a Wi-Fi hotspot or facility's broadband.

will create a private, secure, wireless network with a robust firewall

Disposable Email

Disposable Email

- Primarily for registration on the web

Disposable Email

- Primarily for registration on the web
- Avoid potential spam

Disposable Email

- Primarily for registration on the web
- Avoid potential spam
- Keep from exposing your email from possible hacking

Disposable Email

Disposable Email

- How does it work?

Disposable Email

- How does it work?
- ghacks.net article on disposable email http://www.ghacks.net/2012/05/29/how-to-use-disposable-email-services-like-a-pro/

Disposable Email

- How does it work?
- ghacks.net article on disposable email http://www.ghacks.net/2012/05/29/how-to-use-disposable-email-services-like-a-pro/
- ghacks.net Excel spreadsheet of services http://cdn.ghacks.net/wp-content/uploads/2012/05/disposable-email-services.xls

Privacy Friendly Search Engines

- DuckDuckGo http://duckduckgo.com
- ixquick https://ixquick.com
- StartPage https://startpage.com

Virtual Private Networks

Reference: lifehacker.com (Sept 5, 2102)
http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs

- Private Internet Access https://www.privateinternetaccess.com
- proXPN http://proxpn.com
- TorVPN http://torvpn.com/information.html
- TorGuard http://torguard.net
- WiTopia https://www.witopia.net
- VPN4all https://www.vpn4all.com

TorrentFreak article (October 7, 2011)

http://torrentfreak.com/which-vpn-providers-really-take-anonymity-seriously-111007/

Anonymity

Tor Project

- Originally designed, implemented and deployed by the US Naval Research Laboratory for UN Navy communications
- Subsequently taken over by the Electronic Frontier Foundation (EFF), now run by the Tor Project, a 501(c)(3) organization
- Tor Project: Anonymity Online (https://www.torproject.org)

Tor Sponsors

- SRI International
- US Department of State Bureau of Democracy, Human Rights and Labor
- National Science Foundation in conjunction with Georgia Tech and Princeton University
- Radio Free Asia
- An anonymous North American ISP
- The Ford Foundation
- Google Summer of Code
- More than 4300 individual donors

What is Tor?

- A network of virtual (encrypted) tunnels designed to allow people to remain anonymous while using the net

- Protects against a form of surveillance know as “traffic analysis”

- Projects include a browser

What is Tor?

- Tor is a "lost in the crowd" approach
- Tor funnels many users' traffic through a small number of "nodes." The traffic coming out of any one node could be from any one of an unknown number of individuals
- Tor is useful for anonymity but problematic for privacy

General Guidelines

General Guidelines

From: http://saneadvice.wordpress.com/2014/03/18/how-to-build-a-secure-online-presence/

General Guidelines

General Guidelines

- Set up two-step authentication on all accounts that provide it. (http://twofactorauth.org)

General Guidelines

- Set up two-step authentication on all accounts that provide it. (http://twofactorauth.org)

- Use Diceware to create secure passwords for all your email accounts. (http://world.std.com/~reinhold/diceware.html)

General Guidelines

- Set up two-step authentication on all accounts that provide it. (http://twofactorauth.org)

- Use Diceware to create secure passwords for all your email accounts. (http://world.std.com/~reinhold/diceware.html)

- Create a unique email address for your most valuable log-ins.

General Guidelines

- Set up two-step authentication on all accounts that provide it. (http://twofactorauth.org)

- Use Diceware to create secure passwords for all your email accounts. (http://world.std.com/~reinhold/diceware.html)

- Create a unique email address for your most valuable log-ins.

- Use a good password utility to create unique, strong passwords for every site you visit.

General Guidelines (continued)

Three Credit Agencies: Experian, Transunion and Equifax

Apple and Amazon give you no choice to store CC info. There are others, but opt-out if you can

General Guidelines (continued)

- Create fake security-question answers.

Three Credit Agencies: Experian, Transunion and Equifax

Apple and Amazon give you no choice to store CC info. There are others, but opt-out if you can

General Guidelines (continued)

- Create fake security-question answers.

- Freeze your accounts with all three credit agencies (Experian, Transunion and Equifax) (http://bit.ly/1cwF1ll)

Three Credit Agencies: Experian, Transunion and Equifax

Apple and Amazon give you no choice to store CC info. There are others, but opt-out if you can

General Guidelines (continued)

- Create fake security-question answers.

- Freeze your accounts with all three credit agencies (Experian, Transunion and Equifax) (http://bit.ly/1cwF1II)

- Don't let Web sites store your credit card info

Three Credit Agencies: Experian, Transunion and Equifax

Apple and Amazon give you no choice to store CC info. There are others, but opt-out if you can

General Guidelines (continued)

- Create fake security-question answers.

- Freeze your accounts with all three credit agencies (Experian, Transunion and Equifax) (http://bit.ly/1cwF1II)

- Don't let Web sites store your credit card info

- Hide your Who-is listings if you own your own domains.

Thursday, May 15, 14

Three Credit Agencies: Experian, Transunion and Equifax

Apple and Amazon give you no choice to store CC info. There are others, but opt-out if you can

General Guidelines (continued)

WEP encryption on wifi is inherently insecure and has been broken easily

Paypal has a good checklist for identity theft.

General Guidelines (continued)

- Set up WPA-2 encryption on your wifi router.

WEP encryption on wifi is inherently insecure and has been broken easily

Paypal has a good checklist for identity theft.

General Guidelines (continued)

- Set up WPA-2 encryption on your wifi router.
- **Never** click links in email.

WEP encryption on wifi is inherently insecure and has been broken easily

Paypal has a good checklist for identity theft.

General Guidelines (continued)

- Set up WPA-2 encryption on your wifi router.
- **Never** click links in email.
- Prepare ahead of time for identity theft or hacking. (https://www.paypal.com/us/webapps/mpp/security/report-identity-theft)

Thursday, May 15, 14

WEP encryption on wifi is inherently insecure and has been broken easily

Paypal has a good checklist for identity theft.