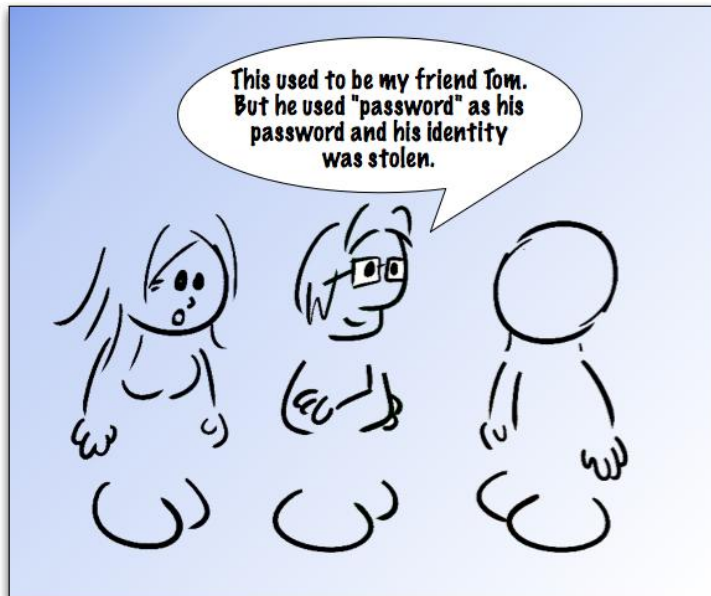


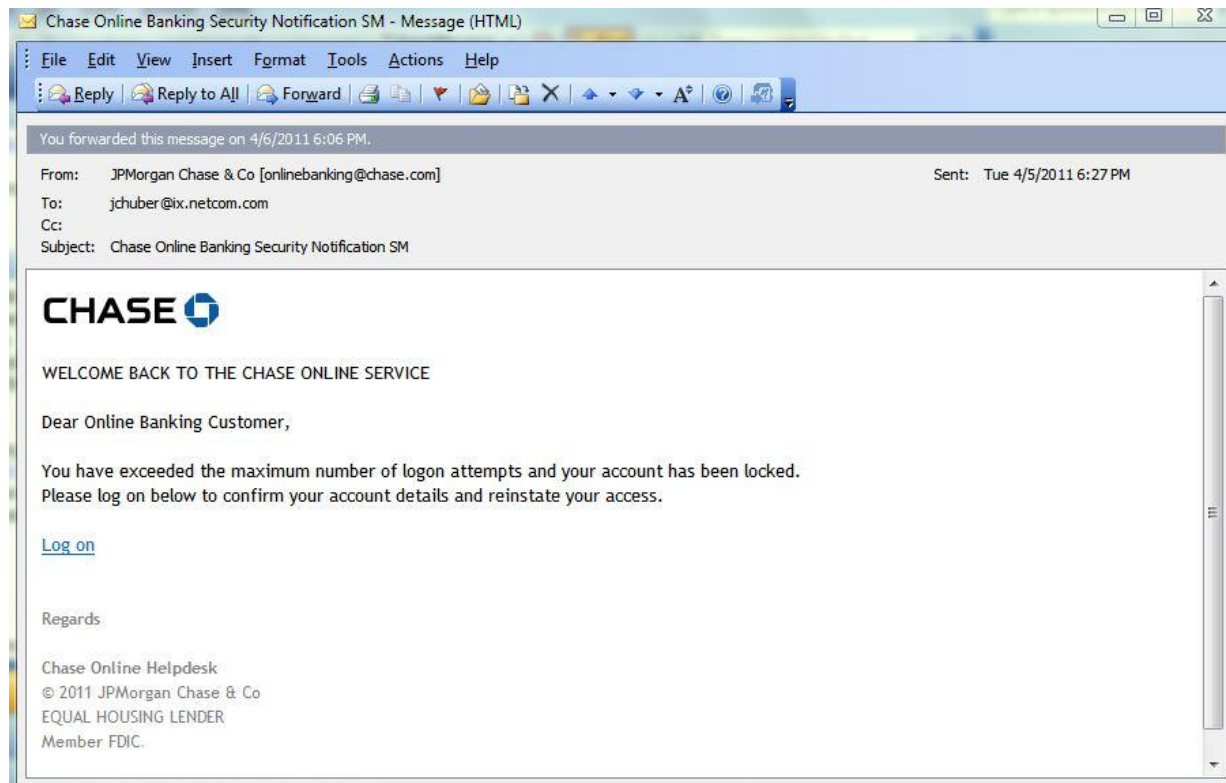
Security, Pins, & Passwords

How to Be Safer on the Wild & Crazy Internet



Security, Pins, & Passwords

- Always keep your Anti Virus up to date
- Never click on links in your email unless you're sure of the sender



Security, Pins, & Passwords

- Look for the lock in the address bar



- Never give remote access to someone you don't know to your computer
- Use Malwarebytes to clean your computer from malware, trojans, etc.
- If you start having problems, act immediately to remedy it

Security, **Pins**, & Passwords

- Most used Pins:

1. **1234 (10%)**

2. **1111**

3. **0000**

4. **1212**

5. **7777**

6. 1004

7. 2000

8. 4444

9. 2222

10. 6969

- Least Used Pin

- 8068



Security, Pins, & Passwords

- Contact your bank or credit card company and change your pin at least twice a year.
- Look around you when you enter your pin to make sure no one is paying unusual attention
- If you lose your card, contract your bank or credit card company immediately
- Check your charges and bank account online often

Security, Pins, & Passwords

The 25 Most Common Passwords of 2012

- | | |
|--------------------|---------------|
| 1. password | 14. sunshine |
| 2. 123456 | 15. master |
| 3. 12345678 | 16. 123123 |
| 4. abc123 | 17. welcome |
| 5. qwerty | 18. shadow |
| 6. monkey | 19. ashley |
| 7. letmein | 20. football |
| 8. dragon | 21. jesus |
| 9. 111111 | 22. michael |
| 10. baseball | 23. ninja |
| 11. iloveyou | 24. mustang |
| 12. trustno1 | 25. password1 |
| 13. 1234567 | |

Security, Pins, & Passwords

- Use passwords of eight characters or more with mixed types of characters
- Avoid using the same username/password combination for multiple websites
- Especially risky is using the same passwords for social, email and financial services
- Do not use basic, personal information
- Keep your passwords in a secret place that isn't easily visible

Security, Pins, & Passwords

A Guide for what a Password should not include

- Your name
- Your spouse's name
- Your parent's name
- Your pet's name
- Your child's name
- Names of close friends
- Names of fantasy characters
- Your boss's name
- Anybody's name
- Computer operating system
- Hostname of computer
- Your phone number
- Your license plate number
- Any part of your SS number
- Anybody's birth date
- Any information about you
- Words such as wizard, guru, etc.
- Any computer user name
- A word in the English dictionary
- A word in a foreign dictionary
- A place
- A proper noun
- Passwords of the same letter
- Simple patterns on the keyboard
- Any words spelled backwards
- Anything beginning or followed by a single digit

Security, Pins, & Passwords

Guidelines of Good Passwords

- Both Upper & Lower Case Letters
- Have Digits and/or Punctuation Characters
- Easy to Remember
- At Least 7 or 8 Characters Long
- Can Be Typed Quickly
- Should Be Changed Every 60 – 90 Days

Security, Pins, & Passwords

- If you're having trouble remembering your passwords, try using a **Password Management Program**
 - Keepass
 - 1Password
 - Password Safe
 - Lockcrypt
 - Roboform
 - LastPass



Security, Pins, & Passwords

- Pros-
 - You don't need to remember dozens of passwords, only one
 - They create strong, secure passwords
 - Each password is unique - and encrypted
 - Works on multiple programs and platforms
 - Manages your passwords for you
 - Stored in the cloud, so they're safe
- Cons-
 - **You're Locked Out if you forget the Master Password**

Security, Pins, & Passwords

- Tonight we're going to review [LastPass](#)

The screenshot shows the LastPass website homepage. At the top, there's a navigation bar with the LastPass logo, a language dropdown set to 'English', and a 'Sign in to LastPass' button. Below this is a secondary navigation bar with links: DOWNLOAD, FEATURES, WHY LASTPASS?, SUPPORT, ABOUT US, and ENTERPRISE. The main content area features a large headline: 'The Last Password You'll Have to Remember!'. Below the headline, it states 'LastPass is a password manager that makes web browsing easier and more secure.' and lists various operating systems and devices it supports: Windows, Mac, Linux, Chrome, Firefox, Safari, Opera, HP webOS, iPhone, Symbian, Android, and BlackBerry. To the right of the headline, there are two prominent yellow buttons: 'Download LastPass' (labeled 'FREE') and 'Get LastPass Premium!' (labeled '\$12 per year - that's \$1 a month!'). At the bottom, there's a grid of six benefits, each with an icon and a brief description: 1. 'it's EASIER' (thumbs up icon) - 'Never forget a password again and log into your sites with a single mouse click.' 2. 'it's SAFER' (shield icon) - 'Protect yourself against phishing scams, online fraud, and malware.' 3. 'it's FREE' (piggy bank icon) - 'No catches or gimmicks. It's free to use on all your computers!' 4. 'it's EVERYWHERE' (globe icon) - 'Automatically synchronizes your data: access it from anywhere at anytime.' 5. 'it's SECURE' (key icon) - 'All of your data is encrypted locally on your PC - only YOU can unlock it.' 6. 'it's MULTI-PLATFORM' (laptop and phone icon) - 'Using a Mac, Windows, or Linux? LastPass works everywhere.'