

# **Identity Theft, Internet Security, and Passwords**

**ASQ 0800**

**Cleveland Section**

**by Wesley R. Richardson**

**March 20, 2013**

# Identity Theft and Internet Security Overview

- **Identity Theft**
- **Internet Security**
- **Passwords**
- **Examples**
- **Deter, Detect, Defend**
- **More information**

# Identity Theft

- **It can't happen to me.**
- **I don't buy anything over the internet.**
- **I don't have any money.**

# Identity Theft

- **How many people have paid for something over the internet?**
- **How many people have given a credit card number over the phone?**
- **How many people have a bank account?**

# Identity Theft

- **How many people have a credit card?**
- **How many people have clicked a link on an e-mail you received?**
- **If you said yes to any of those questions, then identity theft can happen to you.**

# Identity Theft

- **The Veterans Administration (VA) had a breach which appeared to put information about millions of veterans at risk**
- **TJX, parent company of T.J. Maxx and Marshalls had a security breach**
- **The FTC fined ChoicePoint \$10 million for failing to adequately secure consumers' data**

## **Cost of Identity Theft**

- **NBC Dateline March 27, 2007 estimated it costs Americans \$5 billion per year**
- **Federal Trade Commission (FTC) estimated \$53 billion in 2003**
- **First Financial estimates in 2005 that 8.9 million Americans were victims, with a total cost of \$56.6 billion**

## Cost of Identity Theft

- Identity theft can take 1-1/2 to 4 years to resolve.
- As a victim, you must prove that you are yourself.
- Dealing with the issue costs not only money, but many hours of your time.

# Primary Types of Identity Theft

- **Credit card fraud (25%)**
- **Phone or utilities fraud (16%)**
- **Bank fraud (16%)**
- **Employment fraud (14%)**
- **Government documents or benefits fraud, including IRS refunds (10%)**
- **Loan fraud (5%)**

# **Identity Theft Act of 1998**

- **Identity Theft and Assumption Deterrence Act of 1998**
- **United States Code, Chapter 47, Title 18, as amended by Public Law 105-318**
- **Makes identity theft a Federal crime**
- **Penalties up to 15 years imprisonment and a maximum fine of \$250,000**
- **It establishes that the person whose identity was stolen is a true victim.**

# Internet Security

- **How can a breach happen?**
- **Bank or credit card company database breach.**
- **You provide information over the telephone or internet to a legitimate business for a transaction, and an inside person uses or sells the information.**

# Internet Security

- You provide the information in response to a phishing e-mail or other scam.
- Someone using information you provided, sets up an online account and takes over your identity.
- Someone gets your information from the trash, or lost or stolen credit card.

# Internet Security

- **Someone hacks into your computer that is connected to the internet.**
- **Someone accesses your computer through your wireless connection.**
- **You use a public computer and a key stroke program records your information and password.**
- **They randomly create your credit card number.**

# Passwords

- **How many people use one or two different passwords for most of your locations?**
- **Can someone give an example of a password, but not your actual password?**

# Passwords

- **Microsoft Password Checker**

<https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx>

- **Password Creator**

Microsoft

# Safety & Security Centre

Computer Security, Digital Privacy, and Online Safety

United Kingdom Change | All Microsoft Sites

Search Microsoft Security



- Home
- Security
- Privacy
- Family Safety
- Resources

- Sitemap
- Get Support
- Sign Up for Newsletter

## PC Security

Security scanners, tools, and safety guidelines for your PC, laptop, or mobile device.

Passwords

Shopping

Fraud

Protect your information

Social networking

Mobile and wireless

Email Print

### I want to...

+ Get a security update, tool, or scan

+ Protect my kids from online risks

+ Protect my computer

+ Protect myself from scams

+ Protect my personal information

- Create strong passwords

- Create strong passwords
- Check your password

## Check your password—is it strong?

Your online accounts, computer files, and personal information are more secure when you use strong passwords to help protect them.

**Test the strength of your passwords:** Type a password into the box.

Password:

Strength:     BEST

**Note** This does not guarantee the security of the password. This is for your personal reference only.

### What is a strong password?

The strength of a password depends on the different types of characters that you use, the overall length of the password, and whether the password can be found in a dictionary. It should be 8 or more characters long.

For tips about how to create passwords that are easy for you to remember but difficult for others to guess, read [Create strong passwords](#).

### About this password checker

Microsoft does not retain information entered into this password checker. The password you enter is checked and validated on your computer. It is not sent over the Internet.

# Passwords

- Which is better?
- buddy13
- Cleveland
- gn(N&9m\$Dd%uC@ePBoiHR

# Passwords

- **buddy13 (13 seconds to crack)**
- **Cleveland (a few seconds)**
- **gn(N&9m\$Dd%uC@ePBoiHR**
- **3 x 10<sup>23</sup> years!**
- **1 x 10<sup>39</sup> permutations**

# Passwords

- Password restore programs can test 75 million passwords per second
- 6 upper and lowercase letters  
 $1.977 \times 10^{10}$  permutations, takes only 3.3 minutes to crack
- 8 upper and lowercase letters  
 $5.346 \times 10^{13}$  permutations, takes 148.5 hours to crack

# Passwords

- **Strong passwords contain at least 14 characters, 21 is preferred**
- **Use a combination of uppercase and lowercase letters, numbers, and special characters  
!@#\$%^&\*()**
- **Do not use words in the dictionary, common places, your SSN, name, birthdate, or mother's maiden name**

# Passwords

- For security questions, do not give real information, such as your mother's maiden name.
- Not Richardson, but Rich47blue3
- For pet's name, not Fluffy, but Fluf96mydg32
- For city, Clev44SoloCuyah

# Passwords

- **Keep multiple backups of your password file.**
- **My password file is password protected with a strong password**
- **Kept in WordPerfect, Adobe and Word formats**
- **Kept on multiple computers, locations, and external drives**

# Passwords

- **Sample password file includes:**
- **Company, website**
- **Username, my e-mail, password**
- **Security questions and answers**
- **Last 4 digits of credit cards there**
- **Date last visited, their phone**

# Examples

- You have set up strong passwords
- What do you do with:

• Chase	• Discover
• PayPal	• Macy's
• NCUA	• Verizon
• Tech Support	• Dr. Ali Ahoefa
• Mystery shopper	

## e-mail Guidelines

- **Do not click on links received in e-mails**
- **Go directly to the site and logon to your account**
- **Watch for words like: unauthorized activity, your account will be closed or suspended, click here to verify your account, you have won**

## e-mail Guidelines

- **If you receive an e-mail that says we noticed unusual activity on your account, and for your protection, have locked the account.**
- **Click here to reactivate your account.**
- **DO NOT CLICK on the link! It is fraudulent.**

# Deter, Detect, Defend

## Deter

- **Shred financial and personal documents (cross-cut shredder)**
- **Protect your Social Security Number**
- **Don't give out personal information by phone, mail or internet, such as bank or credit card information**

## Deter

- **Never click on links in e-mail, instead go to the web address.**
- **Use firewalls, anti-spyware and anti-virus software. (I recommend Norton 360)**
- **Use strong passwords, do not use your name, birth date, part of your SSN, or mother's maiden name.**

## Deter

- **Do not use Internet Explorer to save your online passwords. Instead use Norton 360 Identity Protection for passwords.**
- **Set Internet Explorer, Tools, Options, Delete Browsing History, and Delete on Exit.**
- **Scan any files or file attachments before loading on your computer.**

## Deter

- **Keep personal information in a secure place at home.**
- **Change your passwords at least every 90 days, or if you detect any unusual activity.**
- **Use different passwords for each account.**
- **Mail bill payments at the post office, and do not place in mailbox**

## Deter

- **Do not click on “remove me” from e-mails, except for legitimate companies.**
- **Do not send credit card information via e-mail, it is not secure.**
- **Do not open file attachments from unknown sources.**

## Deter

- **Set Word and Excel (File, Options, Trust Center, Settings, Disable all macros with notification.**
- **Once a week run Windows Update and anti-virus software updates.**
- **Verify charities through Better Business Bureau before donating, do not commit over the phone, you initiate the contact.**

## Detect

- **Be alert for bills that do not arrive when expected, unexpected credit card statements, or letters about purchases not made.**
- **Check your credit reports at least once a year. Link to free reports:  
<http://www.annualcreditreport.com>**
- **Equifax, Experian, TransUnion**

# Detect

- **Avoid:**
- **<http://www.creditreport.com>**
- **<http://www.freecreditreport.com>**
  
- **And many similar sites, they are not free. Most want some type of monthly fee.**

## Detect

- **Once a week, or at least once a month, check your bank and credit card accounts online to verify transactions and personal information.**
- **Use account alerts to notify you of activity over limits you set.**

## Detect

- **Make sure you have passwords for all bank accounts and credit cards.**
- **This includes store credit cards like Home Depot, Lowes, Sears, Kohls.**
- **Keep a copy of all account numbers, expiration dates, and their phone numbers in your password protected file. This is in case you lose a card or cards.**

## Detect

- **We set our credit card alerts via e-mail for minimum values allowed.**
- **Watch for charge patterns of \$0 or \$1, then around \$200, the next one will be \$2,000 to \$3,000.**
- **Watch for company names or locations you do not recognize.**
- **Call the credit card company immediately.**

## **Defend – If you are a Victim**

- **As soon as you suspect identity theft: Place a “fraud alert” on your credit reports. This also entitles you to free copies of your credit report. Then contact the following:**
- **Equifax (800) 525-6285**
- **Experian (888) 397-3742**
- **TransUnion (800) 680-7289**

## **Defend – If you are a Victim**

- **Close any accounts that have been tampered with or established fraudulently.**
- **Contact the security or fraud department of each compromised account.**
- **Follow-up in writing, with copies of supporting documents**
- **File a police report**

## Defend – If you are a Victim

- Report the theft to the Federal Trade Commission (FTC)
- <http://www.ftc.gov/idtheft>
- (877) 438-4338
- (877) ID-THEFT
- Use the ID Theft Affidavit to support your claims

## More Information

- **File includes key web sites:**
- **Federal Trade Commission (FTC)**
- **AnnualCreditReport.com, Consumer**
- **Experian, Equifax, TransUnion**
- **Federal Bureau of Investigation (FBI)**
- **USA.gov, Identity Theft Act of 1998**
- **Internet Crime Complaint Center (ICCC)**
- **Better Business Bureau (BBB)**
- **Identity Theft Assistance Center (ITAC)**
- **International Association of Privacy Professionals (IAPP)**

**Questions?**