Banking Security

Presented by

Craig Huntington

Alliance Association Financial Services

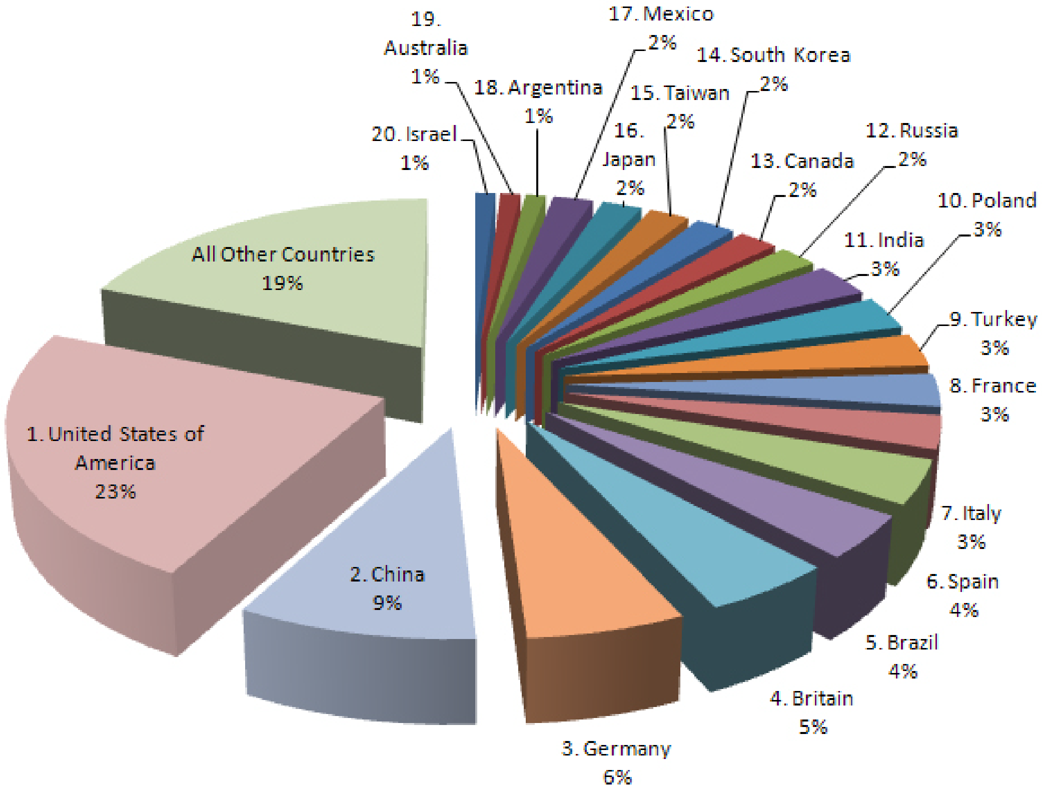
ALLIANCE
Association
Financial
Services™

$142 billion	World’s marijuana market
$85 billion	World’s cocaine market
$61 billion	World’s heroin market
$114 billion	World’s cybercrime market
$274 billion	Time lost due to cybercrime

ALLIANCE
Association
Financial
Services™

CYBERCRIME

IT IS EVERYWHERE!



Cybercrime: Top 20 Countries

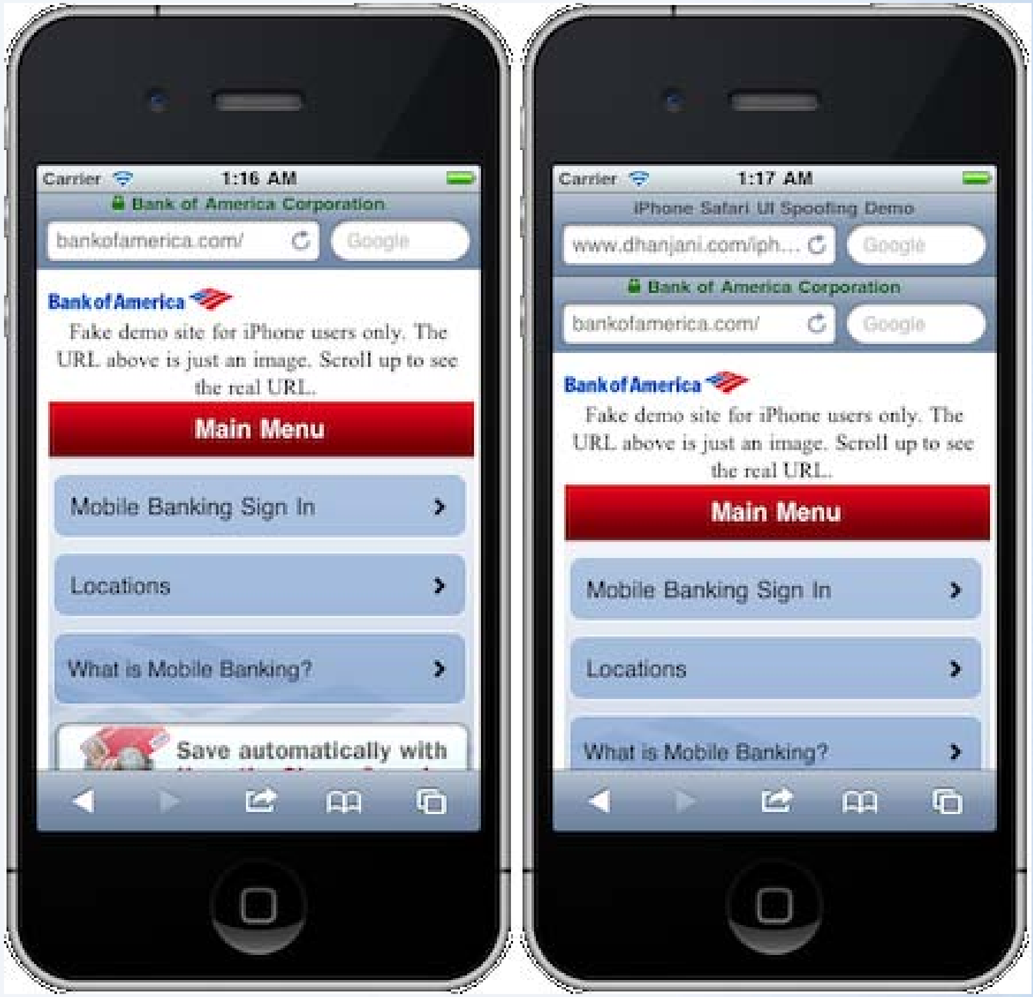
ALLIANCE Association Financial Services™

Data from 2009

69%

ALLIANCE
Association
Financial
Services™

SPOOFING



Fake demo site for iPhone users only. The URL above is just an image. Scroll up to see the real URL.

Fake demo site for iPhone users only. The URL above is just an image. Scroll up to see the real URL.

ALLIANCE
Association
Financial
Services™

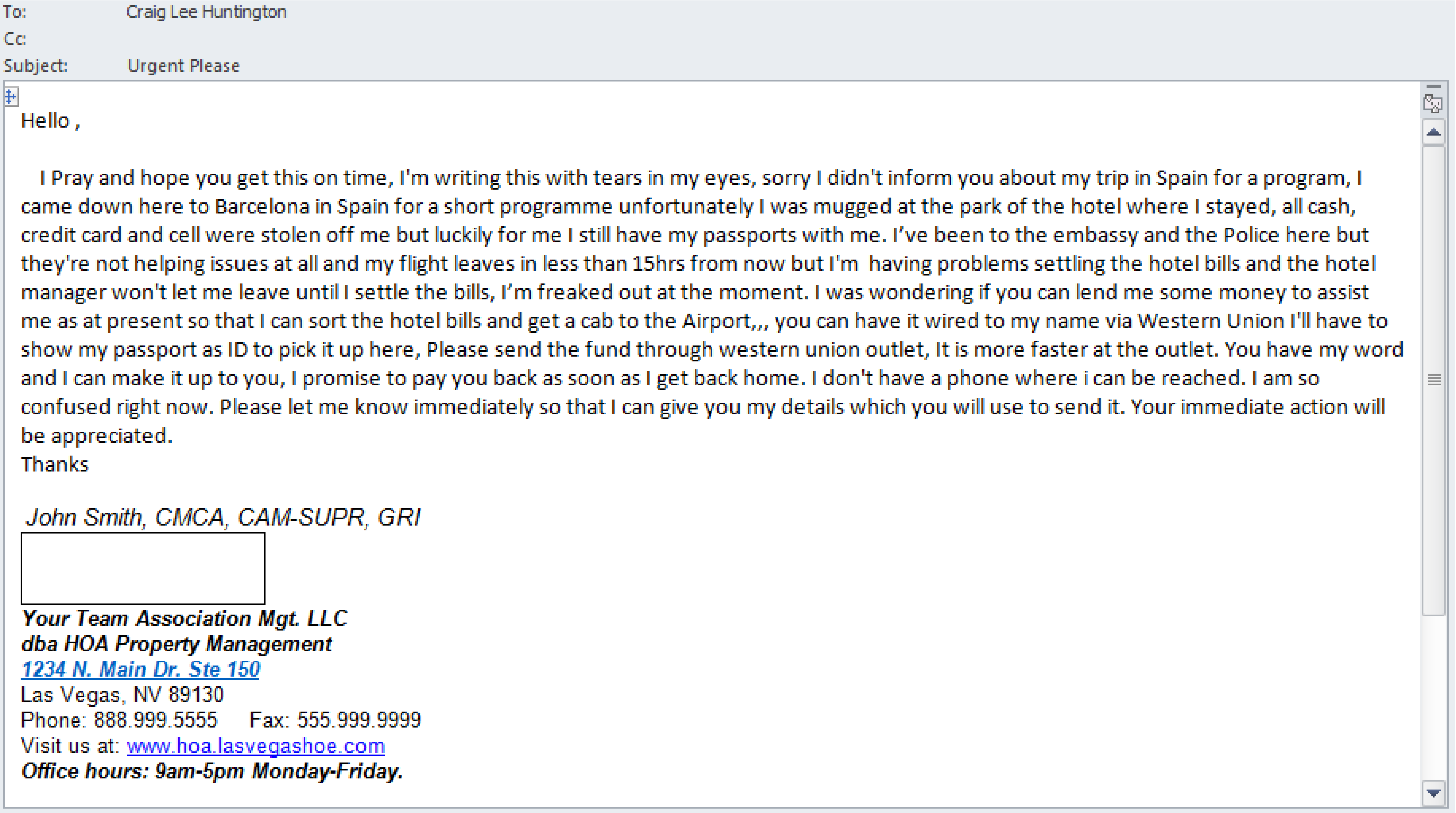
Spoof Email (Phishing)

Phishing emails are an attempt by thieves to lure you into divulging personal and financial information, for their profit. They pretend to be from well-known legitimate businesses, and increasingly look as if they actually are. They use clever techniques to induce a sense of urgency on your part so that you don't stop to think about whether they are legitimate or not. You can learn to know what to look for and where to report these scams when you find them.

6 Ways to Recognize Phishing

1. **Generic Greeting**
   For example, “Dear Customer”.
2. **Sense of urgency.**
   May include an urgent warning requiring immediate action.
3. **Account status threat.**
   May include a warning that your account will be terminated unless you reply.
4. **Forged email address.**
   The sender’s email address may be forged, even if it looks legitimate.
5. **Forged links to Web sites.**
   There is often a link to a Website to “fix” the problem. These are usually forged.
6. **Requests for personal information**.
   Asking for login and password info, either in email or via the link.

ALLIANCE
Association
Financial
Services™



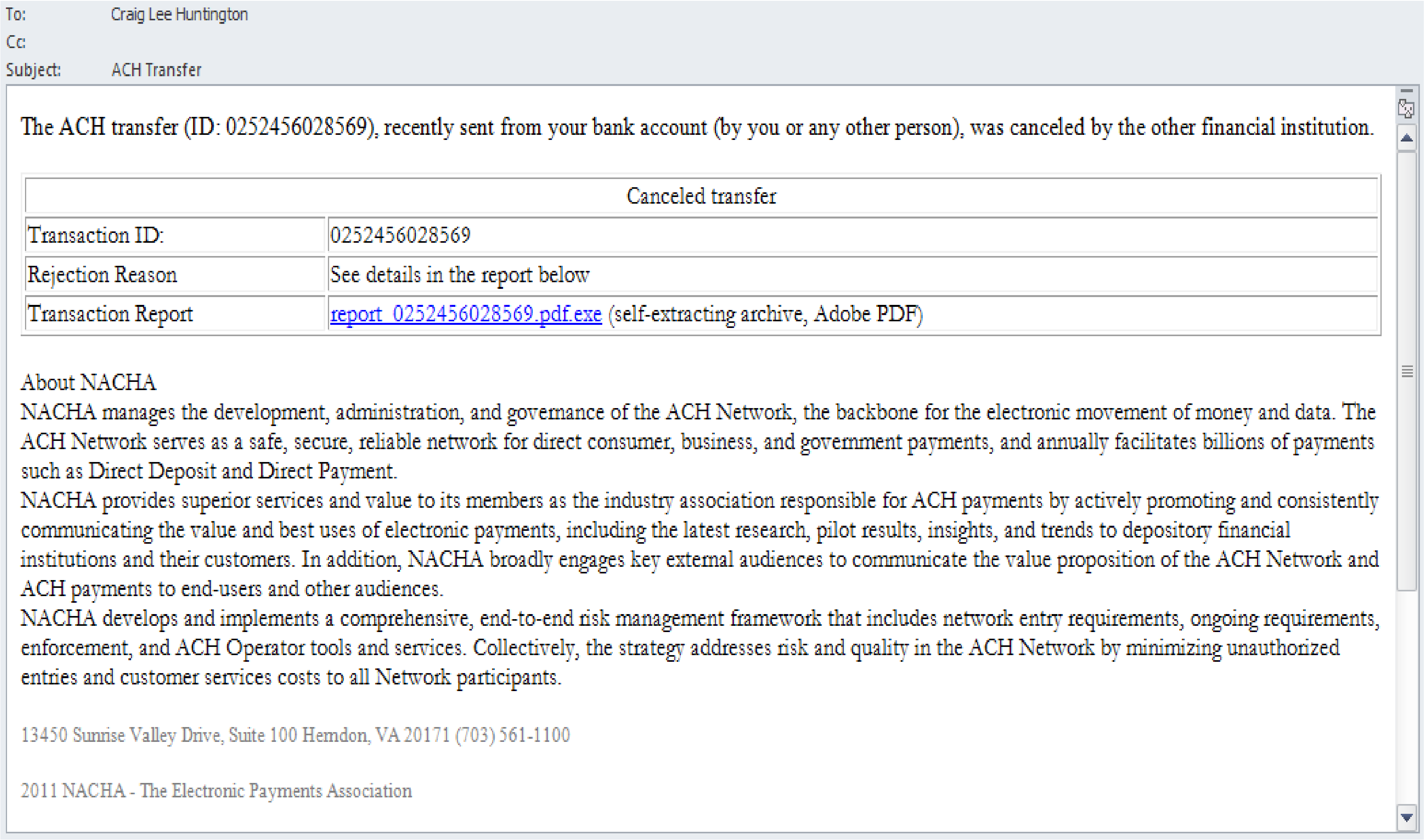
To: Craig Lee Huntington
Cc:
Subject: Urgent Please

Hello ,

I Pray and hope you get this on time, I'm writing this with tears in my eyes, sorry I didn't inform you about my trip in Spain for a program, I came down here to Barcelona in Spain for a short programme unfortunately I was mugged at the park of the hotel where I stayed, all cash, credit card and cell were stolen off me but luckily for me I still have my passports with me. I've been to the embassy and the Police here but they're not helping issues at all and my flight leaves in less than 15hrs from now but I'm having problems settling the hotel bills and the hotel manager won't let me leave until I settle the bills, I'm freaked out at the moment. I was wondering if you can lend me some money to assist me as at present so that I can sort the hotel bills and get a cab to the Airport,,, you can have it wired to my name via Western Union I'll have to show my passport as ID to pick it up here, Please send the fund through western union outlet, It is more faster at the outlet. You have my word and I can make it up to you, I promise to pay you back as soon as I get back home. I don't have a phone where i can be reached. I am so confused right now. Please let me know immediately so that I can give you my details which you will use to send it. Your immediate action will be appreciated.
Thanks

John Smith, CMCA, CAM-SUPR, GRI

Your Team Association Mgt. LLC
dba HOA Property Management
1234 N. Main Dr. Ste 150
Las Vegas, NV 89130
Phone: 888.999.5555 Fax: 555.999.9999
Visit us at: www.hoa.lasvegashoe.com
Office hours: 9am-5pm Monday-Friday.



To: Craig Lee Huntington
Cc:
Subject: ACH Transfer

The ACH transfer (ID: 0252456028569), recently sent from your bank account (by you or any other person), was canceled by the other financial institution.

Canceled transfer	
Transaction ID:	0252456028569
Rejection Reason	See details in the report below
Transaction Report	report_0252456028569.pdf.exe (self-extracting archive, Adobe PDF)

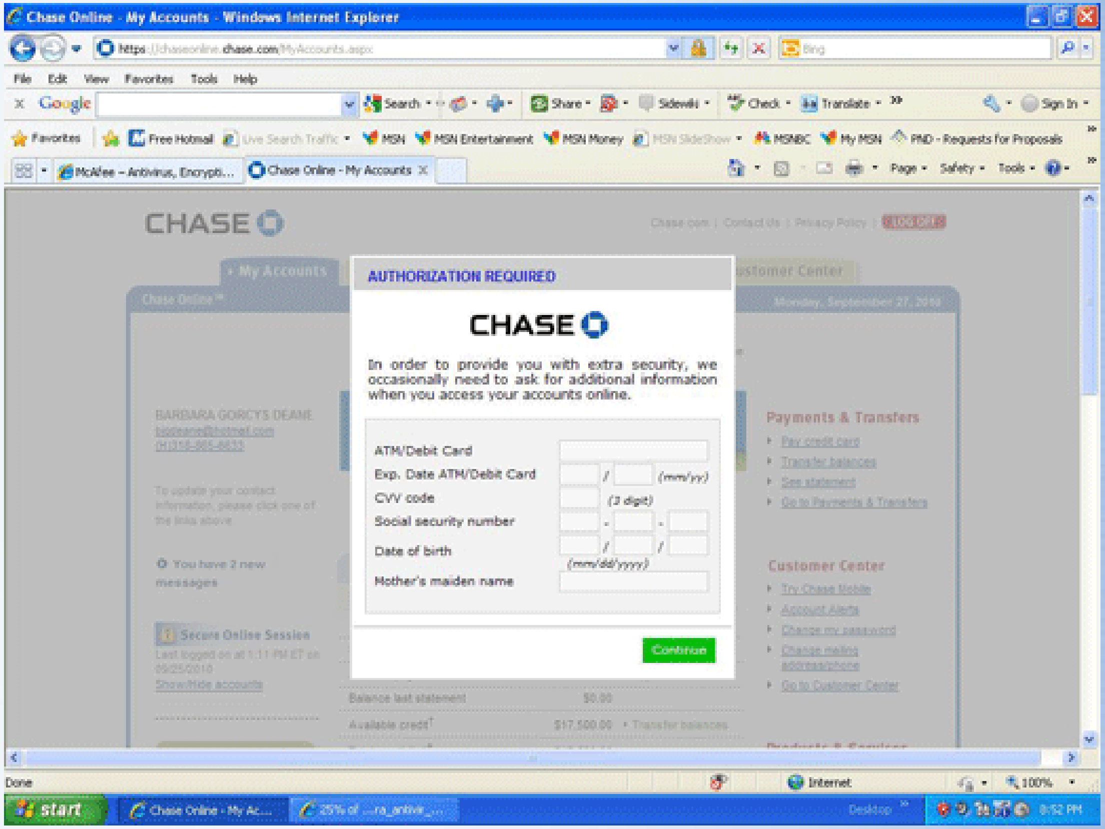
About NACHA
NACHA manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data. The ACH Network serves as a safe, secure, reliable network for direct consumer, business, and government payments, and annually facilitates billions of payments such as Direct Deposit and Direct Payment.
NACHA provides superior services and value to its members as the industry association responsible for ACH payments by actively promoting and consistently communicating the value and best uses of electronic payments, including the latest research, pilot results, insights, and trends to depository financial institutions and their customers. In addition, NACHA broadly engages key external audiences to communicate the value proposition of the ACH Network and ACH payments to end-users and other audiences.
NACHA develops and implements a comprehensive, end-to-end risk management framework that includes network entry requirements, ongoing requirements, enforcement, and ACH Operator tools and services. Collectively, the strategy addresses risk and quality in the ACH Network by minimizing unauthorized entries and customer services costs to all Network participants.

13450 Sunrise Valley Drive, Suite 100 Herndon, VA 20171 (703) 561-1100

2011 NACHA - The Electronic Payments Association

PHISHING

Phishing is the luring of a victim to a fake website that appears to be the same as the real or trusted website from a legitimate company.


Chase Online - My Accounts - Windows Internet Explorer
https://chaseonline.chase.com/MyAccounts.aspx
File Edit View Favorites Tools Help
CHASE
My Accounts
Customer Center
Payments & Transfers
Done
Internet
100%
start

AUTHORIZATION REQUIRED

CHASE

In order to provide you with extra security, we occasionally need to ask for additional information when you access your accounts online.

ATM/Debit Card
Exp. Date ATM/Debit Card / (mm/yy)
CVV code (3 digit)
Social security number - -
Date of birth / / (mm/dd/yyyy)
Mother's maiden name

Continue

ALLIANCE Association Financial Services

ADDITIONAL THREATS

KEY LOGGERS

- Malicious programs that hackers can install on your computer and track every key stroke.
- Can obtain login credentials

MAN-IN-THE-MIDDLE

- Attacker can read, insert, and modify at will any messages between two parties without them knowing.

ALLIANCE Association Financial Services™

Statistics from IC3

- IC3 is the Internet Crime Complaint Center, which was a program developed by NW3C/BJA and the FBI in 2000.
- According to their 2010 annual report, IC3 received it's 2 millionth complaint

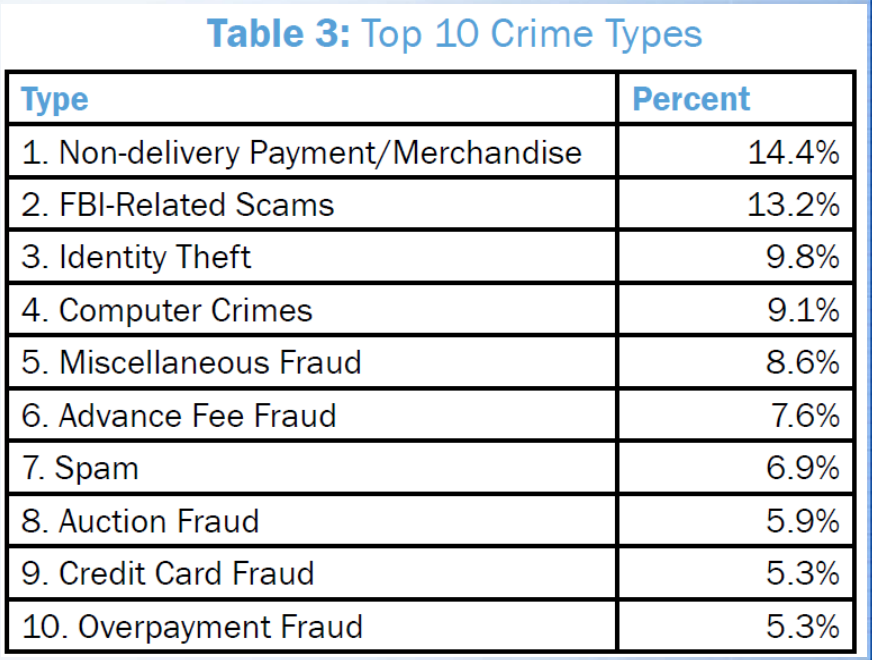
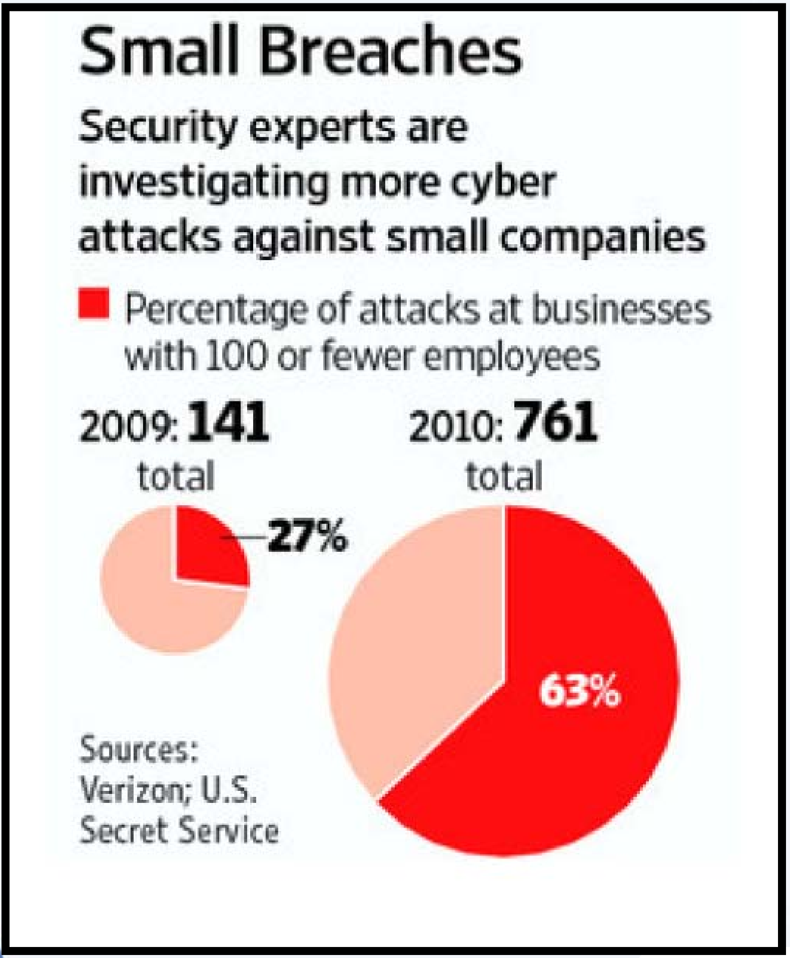


Table 3: Top 10 Crime Types

Type	Percent
1. Non-delivery Payment/Merchandise	14.4%
2. FBI-Related Scams	13.2%
3. Identity Theft	9.8%
4. Computer Crimes	9.1%
5. Miscellaneous Fraud	8.6%
6. Advance Fee Fraud	7.6%
7. Spam	6.9%
8. Auction Fraud	5.9%
9. Credit Card Fraud	5.3%
10. Overpayment Fraud	5.3%

Attacks Shift to Small Businesses



Small Breaches

Security experts are investigating more cyber attacks against small companies

Sources: Verizon; U.S. Secret Service

"Who would want to break into us?"

-Joe Angelastri

- City Newsstand in Chicago was the victim of a cyber attack that has left the owner out $22,000

Why is Security So Important for Small Businesses?

Security threats evolving

- A laptop is stolen every 53 seconds[1]
- 75% of SMB have experienced two or more cyber attacks in a twelve month period[2]

Security practices not keeping pace

- Nearly 50% of small businesses do not have a plan to deal with IT disruptions[3]
- Only 23% of small businesses backup data daily[3]

Increased cost of lost data

- On average, small businesses experience three IT disruptions a year[4]
- 50% of small businesses have lost critical data within the last year[3]

ALLIANCE Association Financial Services

[1] "Notebook Total Cost of Ownership: 2008 Update," Gartner, February 2008 (www.Gartner.com)
[2] Symantec, "2010 SMB Information Protection Survey,
[3] Source: Rubicon Consulting, 2009, US based survey
[4] Source: SMB Disaster Preparedness Survey, Symantec, Q3 2009

Additional Articles

- http://www.infosecisland.com/blogview/6481-Small-Businesses-Hammered-By-Cybercrime.html
- http://www.msnbc.msn.com/id/41742303/ns/business-consumer_news/t/cybercrooks-target-vulnerable-small-businesses/

HOA Specific Fraud Crimes

Koger Management

Aurora Management

Arrow Management

ALLIANCE Association Financial Services

How do you protect yourself and your HOA’s Money?

- Develop Internal Controls
- Utilize One-Time Passcodes
- Don’t Initiate Wires
- Positive Pay
- ACH Filtering
- Secure/Strong Passwords
- Protect Your Computer/Emails/ Mobile Phones

ALLIANCE Association Financial Services

Internal Controls

- Use a separate computer for online banking
- Establish strong passwords that are not easy to figure out, use uppercase, lowercase, and numeric characters
- Change your passwords every 60 days
- Do not share login credentials with other employees in your office
- Review your account balances on a regular basis
- Utilize Auto Reconciliation

One-Time Passcodes

Text/Email/Voice

Key Fobs

~~WIRES~~

DON'T DO THEM!

ALLIANCE
Association
Financial
Services™

Positive Pay

- Specific formatted file
- Upload to the banks online banking site
- File utilized for processing
- All checks not listed on the file will be rejected
- Customer will be notified and asked if the check should be returned or paid

ACH Filtering

- Allows companies to denote what accounts can accept ACH payments.
- Accounts can be established to accept debits only, credits only, or debits and credits

Developing Secure Passwords

- **Length.** Make your passwords long with eight or more characters.
- **Complexity.** Include letters, punctuation, symbols, and numbers. Use the entire keyboard, not just the letters and characters you use or see most often. The greater the variety of characters in your password, the better. However, password hacking software automatically checks for common letter-to-symbol conversions, such as changing "and" to "&" or "to" to "2."
- **Variation.** To keep strong passwords effective, change them often. Set an automatic reminder for yourself to change your passwords on your email, banking, and credit card websites about every three months.
- **Variety.** Don't use the same password for everything. Cybercriminals steal passwords on websites that have very little security, and then they use that same password and user name in more secure environments, such as banking websites.

ALLIANCE Association Financial Services™

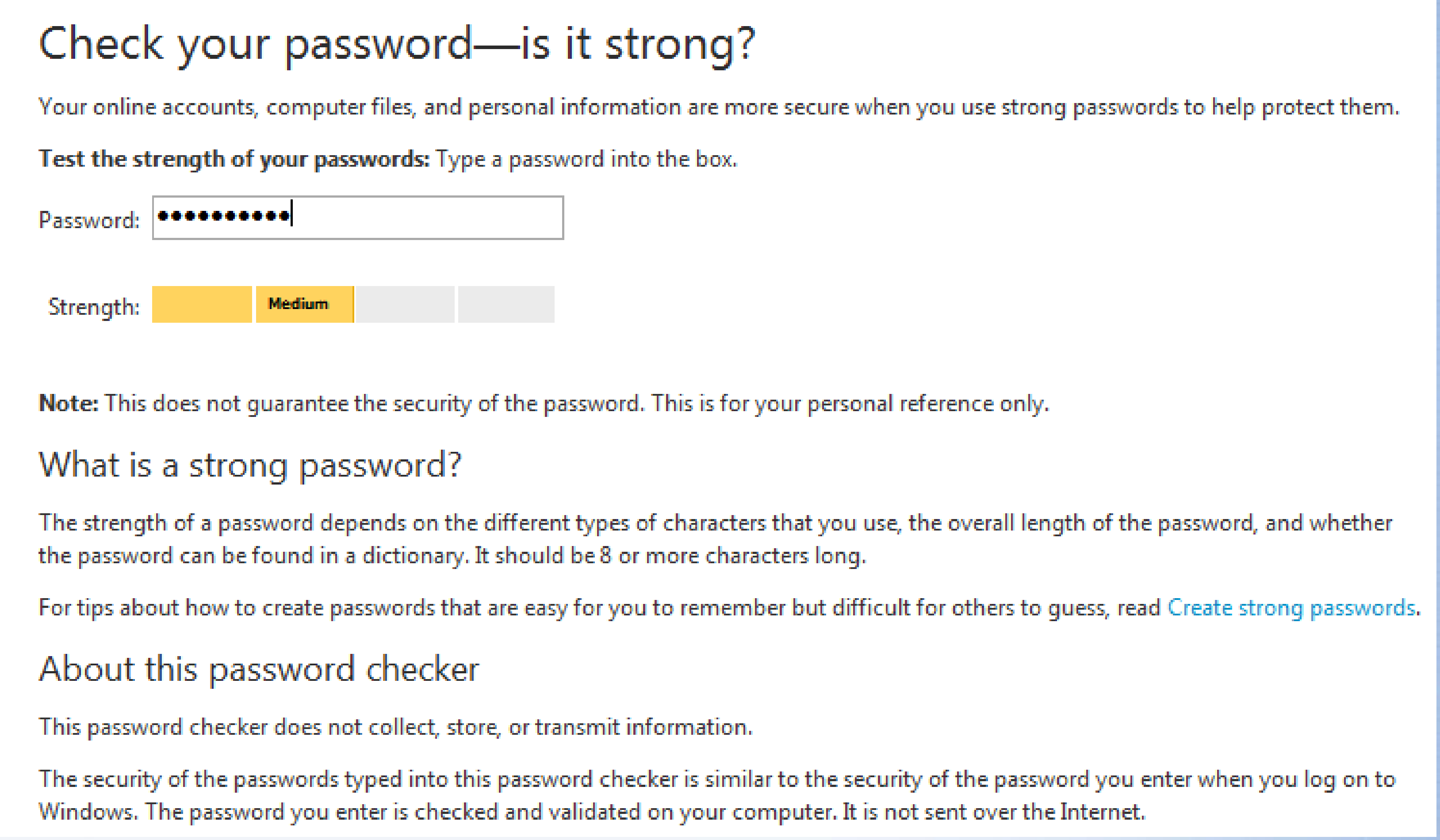
Creating a Strong Password

What to do	Example
Start with a sentence or two.	Complex passwords are safer.
Remove the spaces between the words in the sentence.	Complexpasswordsaresafer.
Turn words into shorthand or intentionally misspell a word.	ComplekspasswordsRsafer.
Add length with numbers. Put numbers that are meaningful to you after the sentence.	ComplekspasswordsRsafer2011.

Avoid creating passwords that use:

- Dictionary words in any language.
- Words spelled backwards, common misspellings, and abbreviations.
- Sequences or repeated characters. Examples: 12345678, 222222, abcdefg, or adjacent letters on your keyboard (qwerty).
- Personal information. Your name, birthday, driver's license, passport number, or similar information.

ALLIANCE
Association
Financial
Services



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: Medium

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

This password checker does not collect, store, or transmit information.

The security of the passwords typed into this password checker is similar to the security of the password you enter when you log on to Windows. The password you enter is checked and validated on your computer. It is not sent over the Internet.

ALLIANCE Association Financial Services

123456
PASSWORD
12345678
1234
pussy
12345
dragon
qWERTY
696969
mustang
letmein
baseball
master
michaEL
FOOTBall
SHADOW
monKEY
ABC123
PASS
fuckME
6969
jordan
HARLEY
RANGER
Iwantu
JENNIFER

CHARLIE
SUPERMAN
ASSHOLE
Biteme
ENTER
ASHLEY
THUNDER
COWBOY
SILVER
RICHARD
FUCKER
ORANGE
MERLIN
MICHELLE
CORVETTE
BIGDOG
CHEESE
MATTHEW
121212
PATRICK
MARTIN
FREEDOM
GINGER
BLOWJOB
nicoLE
SPARKY
YELLOW

COMPUTER
AMANDA
WIZARD
xxxxxxxx
money
PHOENIX
mickEY
BAILEY
Knight
iceman
TIGERS
PURPLE
ANDREA
HORNY
DAKOTA
aaaaaa
PLAYER
SUNSHINE
MORGAN
STARWARS
BOOMER
COWBOYS
EDWARD
CHARLES
GIRLS
booboo
COFFEE
xxxxxx
bulldog

MAVERICK
CHICAGO
JOSEPH
DiabLo
SEXSEX
hARDCORE
666666
Willie
WELCOME
CHRIS
PAnther
YAMAHA
JUSTIN
BANANA
DRIVER
MARINE
AngELS
FISHING
DAVID
MADDOG
HOOTERS
WILSON
BUTTHEAD
DENNIS
FUCKING
CAPTAIN
bigdick
chester

GOLF
BOND007
BEAR
TIGER
DOCTOR
GATEWAY
GATORS
ANGEL
JUNIOR
THX1138
PORNO
BADBOY
DEBBIE
SPIDER
MELISSA
BOOGER
1212
FLYERS
FISH
PORN
MATRIX
TEENS
SCOOBY
JASON
WALTER
CUMSHOT
BOSTON
BRAVES
YANKEE

DONALD
BIGDADDY
BRONCO
PENIS
VOYAGER
RANGERS
BIRDIE
TROUBLE
WHITE
TOP GUN
BIGTITS
BITCHES
GREEN
SUPER
QAZWSX
MAGIC
LAKERS
RACHEL
SLAYER
SCOTT
2222
ASDF
VIDEO
LONDON
7777
MARLBORO

PRINCE
BEACH
AMATEUR
7777777
MUFFIN
REDSOX
STAR
TESTING
SHANNON
MURPHY
FRANK
HANNAH
DAVE
EAGLE1
11111
MOTHER
NATHAN
RAIDERS
STEVE
FOREVER
ANGELA
iPER
0U812
JAKE
LOVERS
SUCKIT
GREGORY
BUDDY
WHATEVER
YOUNG

GIANTS
BOOTY
BLONDE
FUCKED
GOLDEN
0000
FIRE
SANDRA
POOKIE
PACKERS
EINSTEIN
DOLPHINS
00000
CHEVY
WINSTON
WARRIOR
SAMMY
SLUT
8675309
ZXCVBNM
NIPPLES
POWER
VICTORIA
ASDFGH
VAGINA
TOYOTA
TRAVIS
HOTDOG
PARIS

ROSEBUD
JAGUAR
GREAT
COOL
COOPER
1313
SCORPIO
MOUNTAIN
MADISON
987654
BRAZIL
LAUREN
JAPAN
NAKED
SQUIRT
STARS
APPLE
ALEXIS
AAAA
BONNIE
PEACHES
JASMINE
KEVIN
MATT
qWERTYUI
DANIELLE
BEAVER
4321
4128

CALVIN
SHAVED
SURFER
Samson
KELLY
PAUL
MINE
KING
RACING
5555
EAGLE
HENTAI
NEWYORK
LITTLE
REDWINGS
Smith
STICKY
cocacola
animal
BRONCOS
private
SKIPPY
MARVIN
BLONDES
ENJOY
GIRL
APOLLO
PARKER
qWERT

8 Steps to Secure Your Computer

Required (*not just Craig's suggestions*)

1. Safely Install Your Computer's Operating System
2. Keep Your Operating System Up To Date
3. Install and Update Anti-Virus Software
4. Use Strong Passwords

Strongly Recommended

5. Enable Firewall Protection
6. Install and Use Spyware Removal Tools
7. Back Up Important Files
8. Enable Screen Saver Passwords

ALLIANCE Association Financial Services

Install and Update Anti-virus Software

If your computer is connected to the Internet or you share files with anyone, **you need anti-virus software.**

How to Get Anti-virus software

- Company
  - You have to buy professional/commercial software.
  - There is no exception if you have financial information, which every computer you work with does.
- Home Use
  - Purchase commercial anti-virus software.
  - Free Windows version for home use by Avast (avast.com).

Keep the virus definitions up to date.

ALLIANCE
Association
Financial
Services™

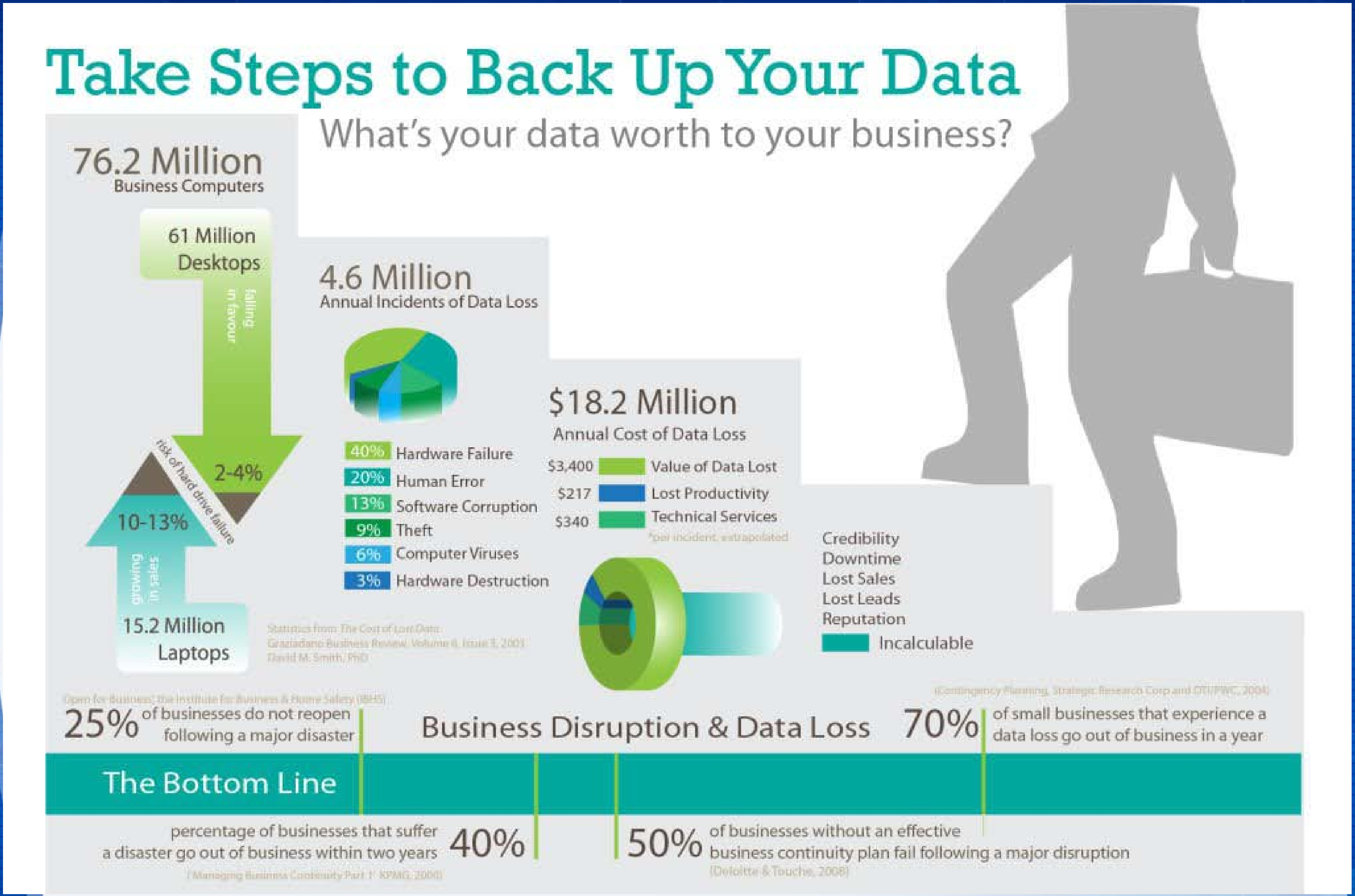
Backups

- Back up your files in the event of a worm or virus attack.
- Daily, Weekly, Monthly
- Store your backup data on external hard disks, DVD's, or CD's.
- Data should be placed in a secure, fireproof location and the data should be encrypted to prevent unauthorized people from having access to your information.

ALLIANCE Association Financial Services™

Take Steps to Back Up Your Data

What's your data worth to your business?



76.2 Million
Business Computers

61 Million Desktops

15.2 Million Laptops

4.6 Million
Annual Incidents of Data Loss

40%	Hardware Failure
20%	Human Error
13%	Software Corruption
9%	Theft
6%	Computer Viruses
3%	Hardware Destruction

Statistics from *The Cost of Lost Data*
Graziadio Business Review, Volume 6, Issue 3, 2003
David M. Smith, PhD

$18.2 Million
Annual Cost of Data Loss

$3,400	Value of Data Lost
$217	Lost Productivity
$340	Technical Services

*per incident, extrapolated

Credibility
Downtime
Lost Sales
Lost Leads
Reputation

🟩	Incalculable

Open for Business, the Institute for Business & Home Safety (IBHS)

25% of businesses do not reopen following a major disaster

Business Disruption & Data Loss

(Contingency Planning, Strategic Research Corp and DTI/PWC, 2004)

70% of small businesses that experience a data loss go out of business in a year

The Bottom Line

percentage of businesses that suffer a disaster go out of business within two years 40%

"Managing Business Continuity Part 1" KPMG, 2000)

50% of businesses without an effective business continuity plan fail following a major disruption

(Deloitte & Touche, 2008)

ALLIANCE Association Financial Services™

Imogoblog.com

Spyware and How to Avoid It.

Spyware is software that is downloaded and installed onto your computer, often without your knowledge. Spyware monitors and shares your information while you browse the Internet.

- Spyware is often installed by you without your knowledge by piggybacking on other software or by tricking you into installing it.
- Some anti-virus software also has anti-spyware capability.
- Anti-spyware Recommendations for Windows
  - **Adaware** (http://www.lavasoftusa.com/default.shtml.en)
  - **Spybot Search and Destroy** (http://www.safer-networking.org/en/home/index.html)
- Spyware is not a major problem for the Mac OS yet. There are a few software companies that are starting to address the issue.
  - **MacScan** (http://macscan.securemac.com/)
  - **NetBarrier X4 Firewall includes Spyware protection** (http://www.intego.com/netbarrier/)

ALLIANCE
Association
Financial
Services™

Email Safety Tips

1. **Do not open** unexpected attachments.
2. Use **Spam Filters**
3. Beware of **Spoof Emails** or **Phishing**.
4. Don’t send **sensitive data** in email.
5. **Avoid** clicking on links in the body of an email message.

   While these links may not be a phishing attempt, they may not go to the site you intend. Unless you are completely comfortable that the email is legitimate, it is best to copy and paste the link or type it in directly in your browser.

ALLIANCE Association Financial Services℠

Tips to Manage Email Attachments

Most common email viruses are spread through email attachments. Attachments are files that are sent along with the message. If an attachment has a virus it is usually spread when you double-click or open the file. You can minimize the risk of getting a virus from an attachment by following a few simple rules.

1. **Do not** open an attachment unless you are expecting it AND you know who it is from.
2. If you receive an attachment from someone you don't know, **delete it immediately without opening it.**
3. Use **anti-virus software** and keep it updated.
4. If you need to send an attachment, contact the recipient and let him/her know you are sending it.
5. Use **spam filters** to block unsolicited email. Many viruses are sent as spam.

ALLIANCE Association Financial Services™

Managing Spam Email

- Adjust Spam Filter to block unwanted e-mails
- Review e-mails in spam folder on a regular basis
- If they are from an unknown person or someone you do not recognize, **DELETE IT!**

ALLIANCE
Association
Financial
Services™

Password Protect Your Smart Phone

- You can and should password protect your smart phone in which you can send and receive email and surf the internet.
- In which you have contact information
- The IPhone, Android, and Blackberry phones have this feature.
- If the phone is lost a third party cannot readily access your data.

Don’t Send Sensitive Data in Email

Although it's convenient to send colleagues sensitive data in email, it is unsafe. Not only is email an insecure way of sending information, you've lost control over that information once you hit the send button.

The Risks of Sending Sensitive Data in Email

1. Sending email is insecure.
2. You are storing sensitive data on your computer.
3. You no longer control the sensitive data.
4. The sensitive data may be sent to others without your knowledge.

Mobile Security

Mobile computing offers the freedom of using your notebook computer or other mobile device in many remote locations. With this freedom also comes greater responsibility to keep the computer and information secure.

Physical Security

- Lock your notebook computer in a safe location when not in use.

Wireless Precautions

WiFi networks are a shared network that makes it easier for others to eavesdrop on your communication.

- Secure Web Browsing
  - Use secure, encrypted sessions.
- Always use a Personal Firewall when on an untrusted network (hotel, conference, etc.)
  - Set the firewall to deny ALL incoming connections.
- Never store **Sensitive Data** on mobile devices unless absolutely necessary.

Implement a security agreement

- Require employees to sign a security agreement to demonstrate that they are active participants in helping to maintain a secure online environment. This agreement also should require employees to report any suspicious online activity or known Internet crime to the proper authorities.
- If fraud or criminal intent is suspected, you should report it to the local law enforcement agencies, the local Federal Bureau of Investigation, Secret Service, or State Attorney General's offices. Some states also require business owners to notify their customers if criminals have had access to customers' unencrypted personal information.

ALLIANCE Association Financial Services™

Vendor Management and Contract Governance

- **Checklist for due diligence; IT security questionnaire**

- **Ideas for contractual provisions (to be referred to attorneys in the legal department)**

- **Insurance clause provisions**

Sample Insurance Clause

“Vendor agrees to purchase and maintain throughout the term of this Agreement technology/professional liability insurance, intellectual property infringement, and data protection liability insurance (cyber liability) covering liabilities for financial loss resulting or arising from acts, errors, or omissions, in rendering [type of service] or in connection with the services provided under this agreement:

- **intellectual property infringement arising out of software and/or content (excluding patent infringement and misappropriation of trade secrets);**
- **breaches of security;**
- **violation or infringement of any right privacy, breach of federal, state, or foreign security and/or privacy laws or regulations including but not limited to [specific regulations];**
- **data theft, damage, destruction, or corruption, including without limitation, unauthorized access, unauthorized use, identity theft, theft of personally identifiable information or confidential corporate information, transmission of a computer virus or other type of malicious code; and participation in a denial of service attack on a third party**

with a minimum limit of [$X,000,000] each and every claim and in the aggregate. Such insurance must address all of the foregoing without limitation if caused by an employee of the Vendor or an independent contractor working on behalf of the Vendor in performing services under this contract. Policy must provide coverage for wrongful acts, claims, and lawsuits anywhere in the world. Insurer must have a Best's rating of [ ] or better. Any material change in the policy or cancellation must be reported to the Client with not less than thirty (30) days prior written notice. The policy must be kept in force during the life of the contract and for [ ] years (either as a policy in force or extended reporting period) after contract termination. Vendor shall provide a Certificate of Insurance in compliance with these requirements and client reserves the right to obtain a copy of the professional liability and data protection liability insurance policy.”

Additional Issues:* *Additional Insured Status, Waivers of Subrogation, Primary, Separation of Insureds, etc.

ALLIANCE
Association
Financial
Services

Whose Responsible?

Bank Not Responsible for Letting Hackers Steal $300K From Customer

- Judge ruled that a bank that allowed hackers to steal more than $300,000 from a customer’s online account isn’t responsible for the lost money--the customer should have done more to protect the account credentials.
- Patco Construction Company, sued Ocean Bank, after discovering that hackers were siphoning about $100,000 per day from its account.
- The hackers had sent a malicious e-mail to employees and installed the Zeus password-stealing program.
- After obtaining Patco’s banking credentials and waiting for its account to fill up with money, the hackers used the credentials to initiate a series of electronic money transfers.
- Nearly $600,000 worth of transfers were made out of the account before Patco realized it had been hacked.
- Ocean Bank, after being notified of the fraud, was able to block about $240,000 in transfers. But Patco was unable to retrieve the rest.

You Don't Think It Will Happen To You?

Make a plan to protect:

- ✓ Yourself
- ✓ Your customers
- ✓ Your accounts

ALLIANCE Association Financial Services

Craig L. Huntington
(888) 734-4567

Purchase at

www.chuntington.com

Or

www.amazon.com

ALLIANCE
Association
Financial
Services™