

Protecting a Better Quality of Life

Presented by:

Patti Broer, BankWest Information Security Administrator

To:



October 28, 2014



Protecting a Better Quality of Life

Our Mission

We are a team of dedicated professionals who partner with others to achieve our vision of affordable housing through

- integrity,
- financial responsibility,
- innovation
- and sustainability.

Protecting a Better Quality of Life

- ❑ Security Awareness
- ❑ Information Security Mindset
 - ❑ Needs to become SECOND NATURE
 - ❑ Needs to be the HEARTBEAT of your job
- ❑ Security Best Practices

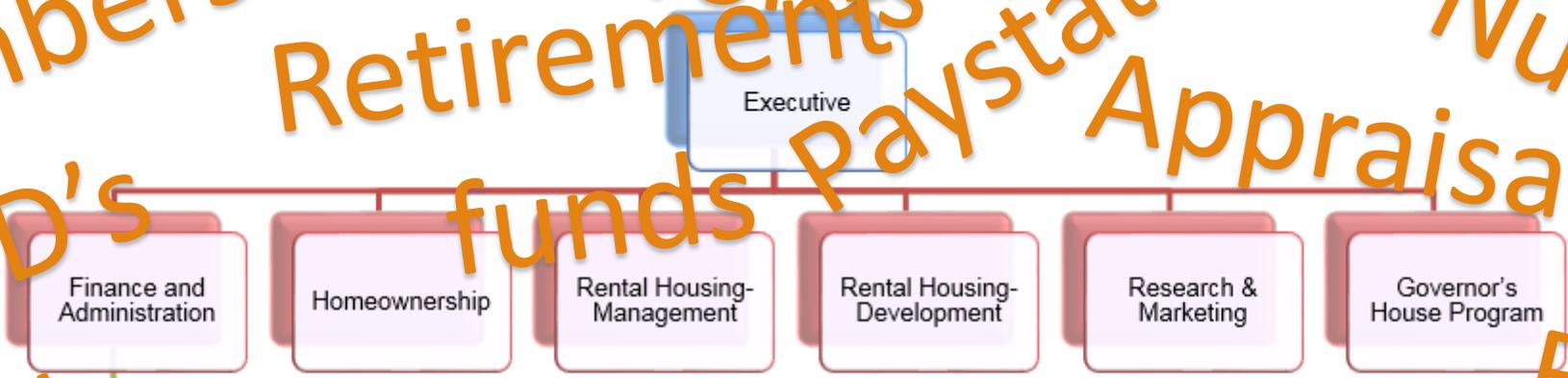
Security Awareness

Insurance
Accounts
numbers

Benefits
Passwords
Retirements

Appraisals
Social Security
Numbers

User ID's



funds

Network
Diagrams
Photo ID

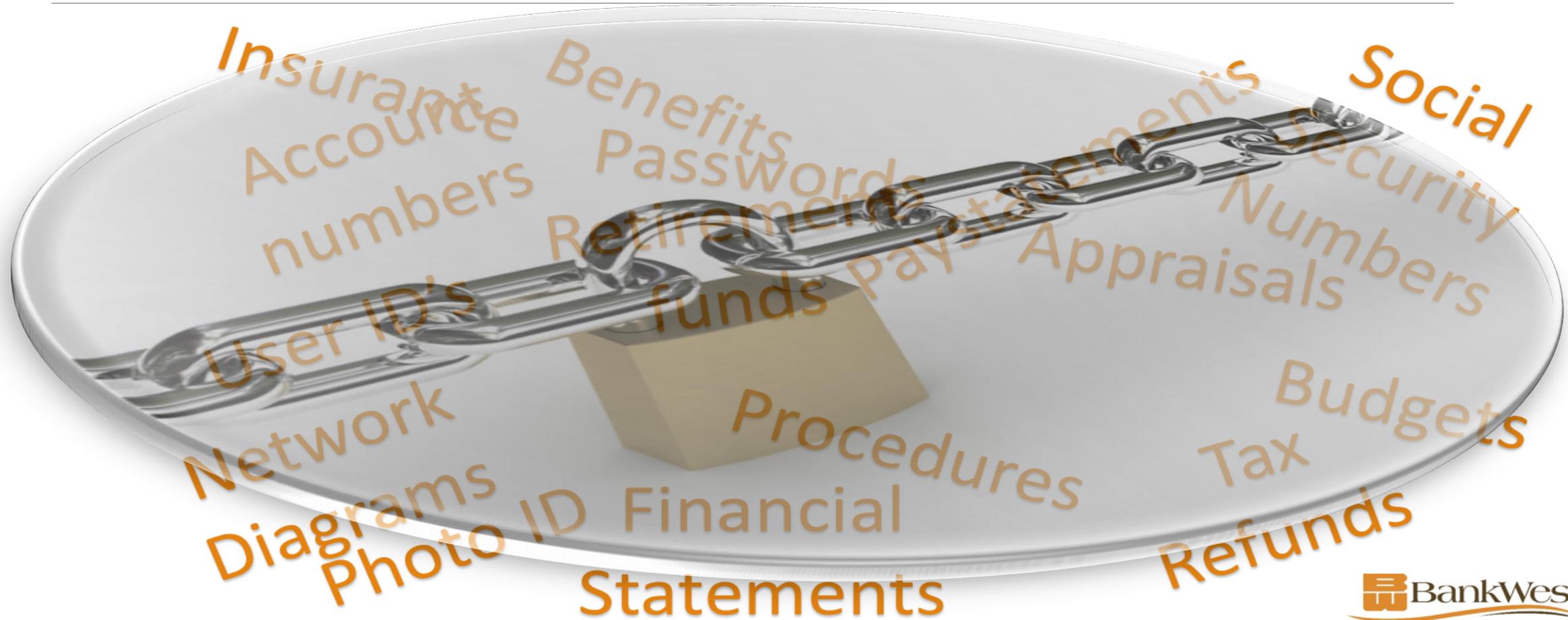
Procedures

Budgets
Tax
Refunds

Financial
Statements

Security Awareness

Information is an Asset **Protect IT!**

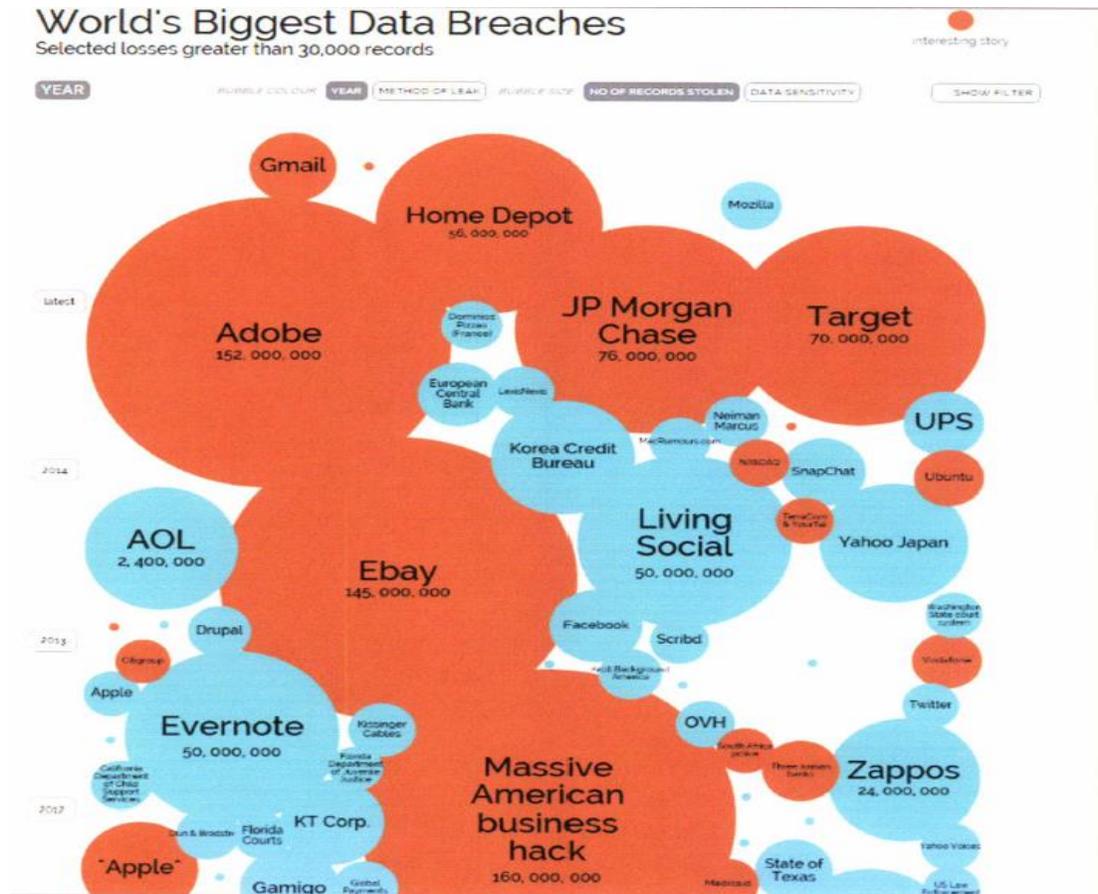


Security Awareness

Protect it from what?

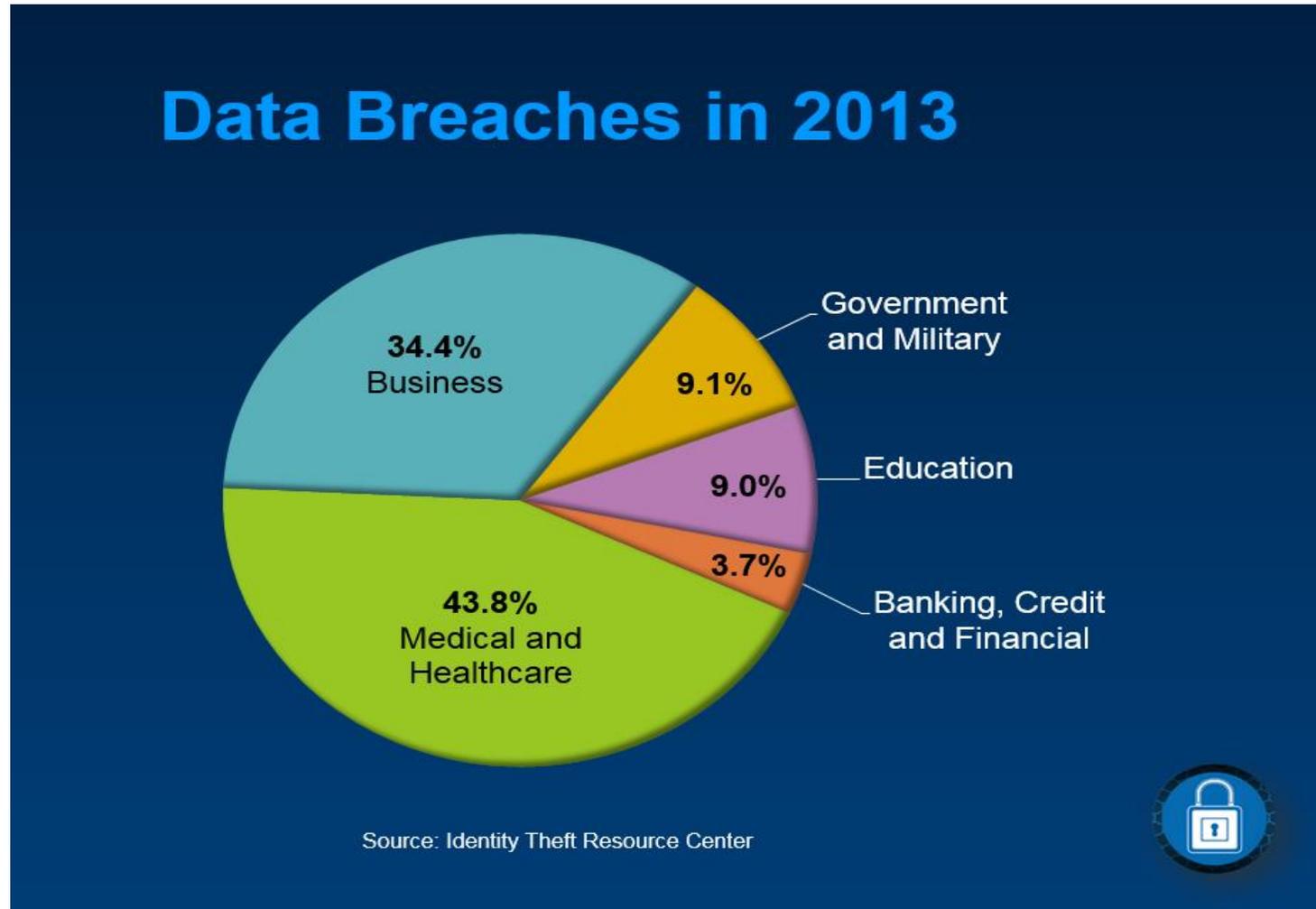
- Identity Theft
- Computer Compromise
- Viruses
- Data Loss/Theft

Security Awareness



[World's Biggest Data Breaches](#)

Security Awareness



Security Awareness

Records Stolen in 2013



1 in 8 Americans
(40 million) had their records stolen in 2013.



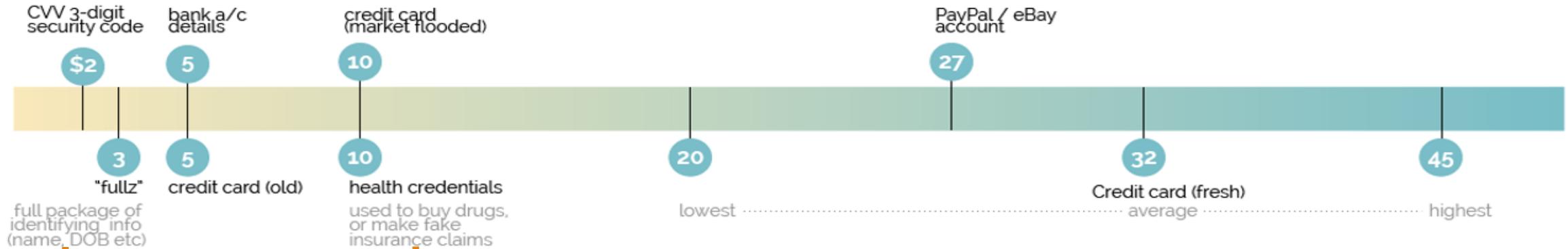
\$100 billion
In losses for the U.S.

Source: CSIS and Intel Security



Security Awareness

How Much is Your Hacked Data Worth? Black market \$ prices



informationisbeautiful.net

data: bit.ly/bigdatabreaches

sources: Holt & Smirnova (2014), Reuters, Globe & Mail, Rand

40 million consumers
X \$3.00 per record
= **\$120 billion or
\$120,000,000,000**

October 15, 2014

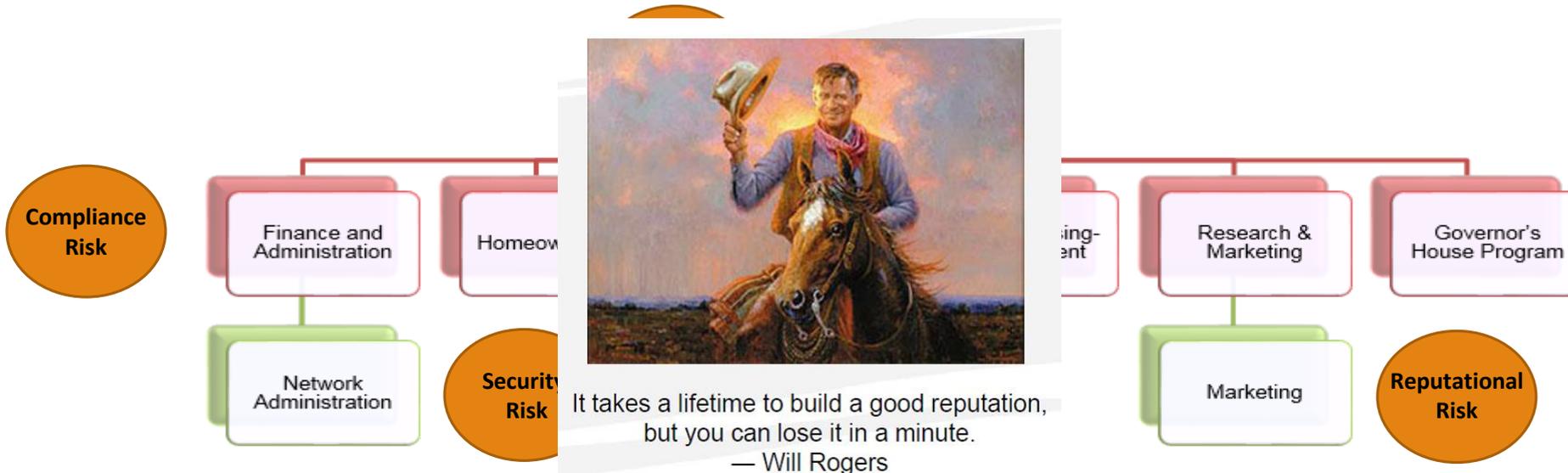
Attorney General warns employers and employees to be cautious of an unemployment insurance benefit scam targeting South Dakota.

- The scenario begins with a scammer filing online for unemployment benefits with the South Dakota Department of Labor and Regulation (DLR).
- The scam artist is filing these claims with accurate personal identifying information including correct name, social security number and date of birth.



Security Awareness

South Dakota Housing Development Authority



Security Awareness

We manage or mitigate risk with CONTROLS

- 1) Anti-Virus and Anti-Spyware
- 2) Secure Internet Connection
- 3) Firewalls
- 4) Install Patches to Correct Security Problems
- 5) Backup Important Data
- 6) Control Physical Access
 - a. Computers
 - b. Network Components
- 7) Secure Wireless Access Points
- 8) Least Access and Least Authority
- 9) Unique User ID's with Strong Passwords
- 10) Employee Training



NISTIR 7621 Small Business Information Security: The Fundamentals

Security Awareness

YOU are the First Line of Defense



Security Awareness



Information Security Mindset

- Information Security Mindset
 - Needs to become SECOND NATURE
 - Needs to be the HEARTBEAT of your job



Information Security Mindset

Expectations about Sensitive Information

Respect and Protect Information for:

- Consumers
- Employer
- Business Partners
- Employees

Information Security Mindset

Our Core Values

PROFESSIONALISM...Displaying leadership, **excellence**, **respect**, empathy and open-mindedness in everything we do.

INTEGRITY...Being **honest** and **ethical**.

ACCOUNTABILITY...**Taking responsibility for our actions** and following through in a consistent, reliable and timely manner.

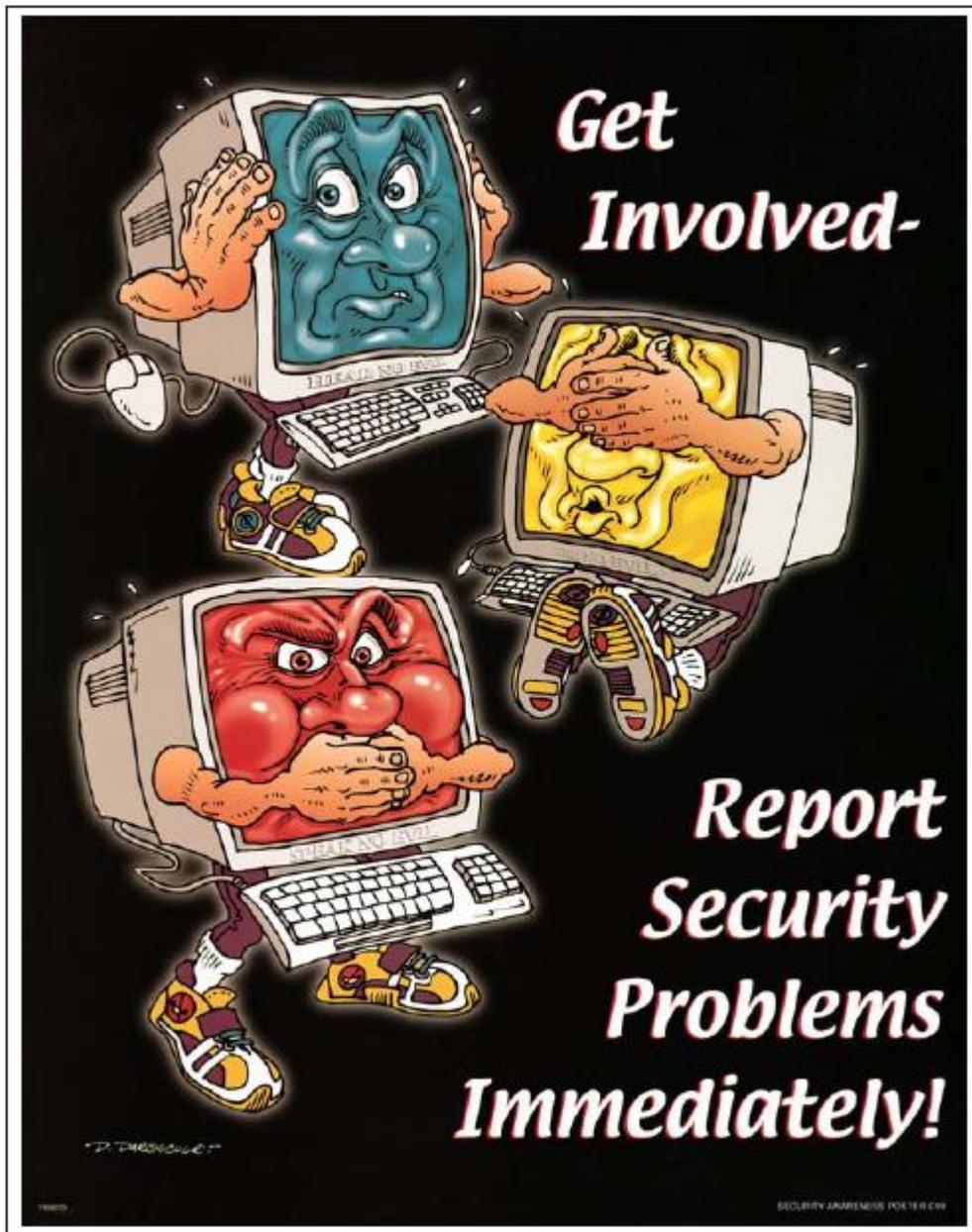
INNOVATION...Creating, embracing and **accepting change** for the betterment of the whole.

COMMUNICATION...**Sharing information**, ideas and opinions with clarity and understanding, **ever mindful of respecting confidentiality**.

TEAMWORK...Supporting one another as we strive to create an exceptional working environment.

Culture of Security





Core Value:

ACCOUNTABILITY...Taking responsibility for our actions and following through in a consistent, reliable and timely manner.



Convenient. Connected. Committed.

Security Best Practices

Internet Activity

- ❑ Don't download software upgrades or files without approval.
- ❑ Limit activity to business purposes
- ❑ Don't accept software free trial offers

Don't get caught in the trap!

Think before you click!



Patti Broer

Meeting start time: 3:37:24 PM 8/20/2012

Duration: 0:00:14

Organizer: patti.broer@bankwest-sd.com

Participants: Patti Broer

Security Best Practices

Physical Access

- ❑ Restrict access and don't allow access to your IT Equipment Rooms without verbal approval from Network Administrators.
- ❑ Protect and restrict access to non-public areas of your building.
- ❑ Lock your computer whenever leaving your work station.
 - ❑ Smartphone Precaution
- ❑ Use caution with USB sticks, if allowed at all.

Security Best Practices

Proper Handling of Physical Documents

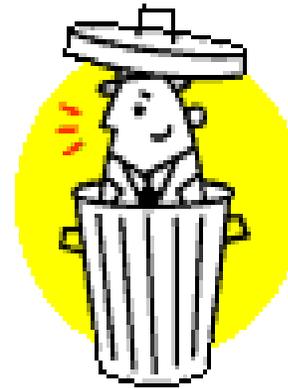
- Think about the confidential information (asset) you're handling.
 - Would you want your information lost in the mail?
 - Would you want your mortgage loan package sitting in your mailbox until you pick up your mail?
 - Would you want it in the street gutter or on the floor of the post office?

- How do you discard confidential and private information?
 - Does it go in the garbage can?
 - Does it get shredded?

Security Best Practices

Proper Handling of Physical Documents

Think about how you'd feel if your confidential papers were somewhere in this pile or thrown in the garbage?



Security Best Practices

Proper Handling of Physical Documents

- ❑ Put documents in a drawer or file cabinet when leaving your desk for any period of time.
- ❑ Don't leave faxes in the machines unattended.
- ❑ Don't leave printed items in the printer.
- ❑ Shred all confidential papers. Don't leave them in personal shred containers overnight.
- ❑ Don't leave sensitive customer information on your desk or computer screen unattended.



Security Best Practices

Core Value

COMMUNICATION...Sharing information, ideas and opinions with clarity and understanding, ever mindful of respecting confidentiality.

Security Best Practices

Use Strong Complex Passwords

- Random sequence of
 - Letters
 - Numbers
 - Special characters
- Changed every 90 days

Use a phrase or compound word:

Building a better quality of life becomes: Babq0L!fe

Single-Family becomes: \$ingl3F@mily

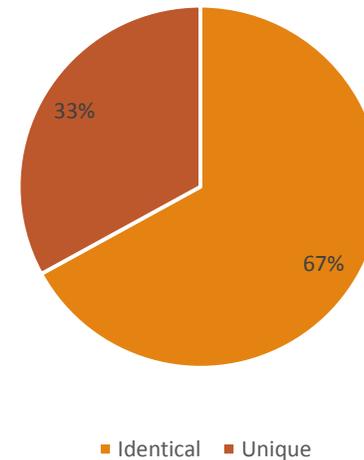
Workmanship becomes: W0rKm@n\$h1p

Security Best Practices

Don't Re-Use Your Password

- ❑ ¹47% of users share both their user ID and password with at least one nonfinancial website
- ❑ “With passwords, the surprise we found was not password complexity, but was people using the same password for several different accounts....Once the bad guys got it, it was very simple to move around [the network].” Lance Spitzner SANS (SysAdmin Audit Network Security) Institute
- ❑ 59% had same between Yahoo and Sony breaches
- ❑ 67% had same between Sony and Gawker breaches

Password Reuse Across Sony and Gawker



¹Secure Banking Solutions, LLC

Security Best Practices

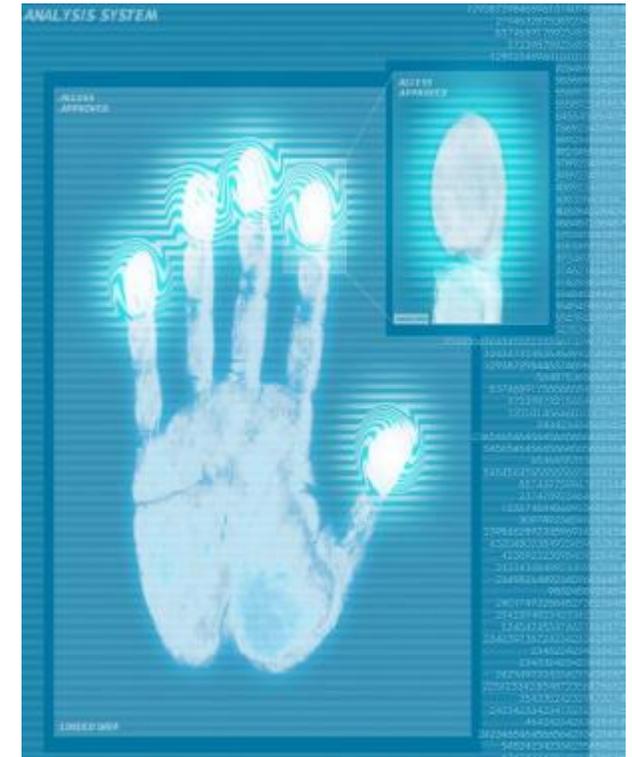
User ID's & Passwords



Security Best Practices

User ID's & Passwords

User ID + Password = Finger Print on your Network
Never share your User ID and Password.



Security Best Practices

Core Value:

INTEGRITY...Being **honest** and **ethical**.

Security Best Practices

Our Core Values

PROFESSIONALISM...Displaying leadership, **excellence**, **respect**, empathy and open-mindedness in everything we do.

INTEGRITY...Being **honest** and **ethical**.

ACCOUNTABILITY...**Taking responsibility for our actions** and following through in a consistent, reliable and timely manner.

INNOVATION...Creating, embracing and **accepting change** for the betterment of the whole.

COMMUNICATION...**Sharing information**, ideas and opinions with clarity and understanding, **ever mindful of respecting confidentiality**.

TEAMWORK...Supporting one another as we strive to create an exceptional working environment.



Security Best Practices

Social Engineering



Simply defined, social engineering is the art of manipulating people into performing actions or divulging confidential information.

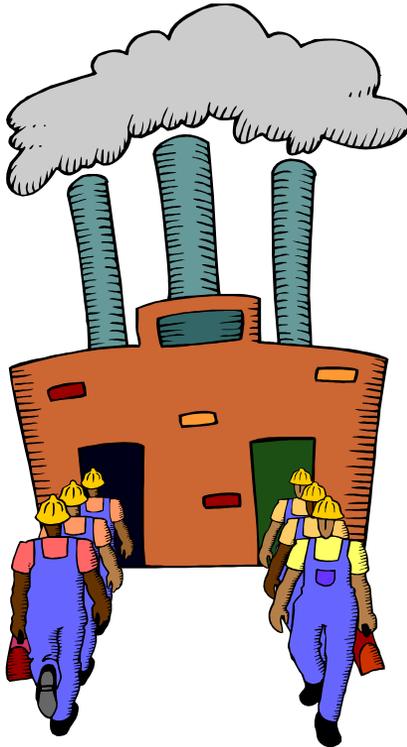
It's similar to a con or fraud and is typically trickery or deception. The sole purpose is to gather information, commit fraud or gain access to computer systems.

Fletch is a 1985 comedy film about an investigative newspaper reporter, Irwin M. Fletcher (Chevy Chase).

- Drug Addict
- Doctor
- Insurance Investigator

Security Best Practices

Social Engineering



Piggy-Backing Tail-Gating

Following employees into non-public areas while pretending to be a vendor, employee, or a customer is one of the methods social engineers use to gain access to unauthorized areas.

This method is called **piggy-backing or tail-gating**.

Security Best Practices

Social Engineering

Poser

Social engineers will enter your facilities posing as a vendor, employee, or a customer and ask to use bathrooms, or wander the facilities.

This method is called **posing**.



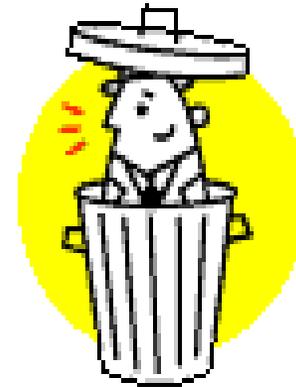
Security Best Practices

Social Engineering

Dumpster Diving

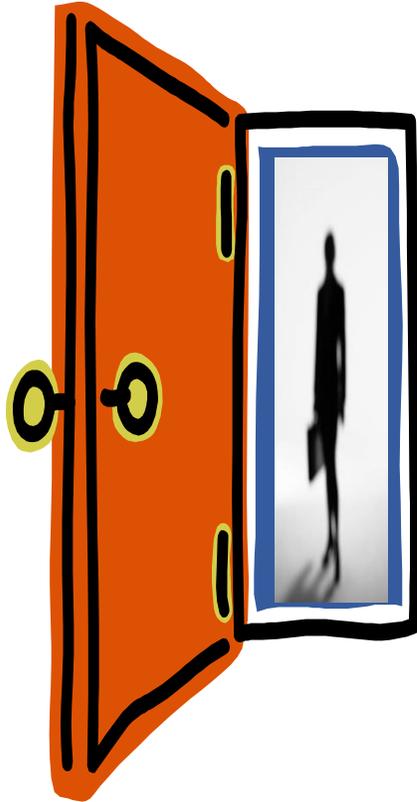
This is where social engineers go through the office garbage hoping to find sensitive confidential customer information that wasn't shredded.

This method is called **dumpster diving**.



Security Best Practices

Social Engineering



Sneaking

Social engineers will find ways to sneak into your facilities through unsecured entrances to gain access to non-public areas.

This method is called **sneaking**.

Security Best Practices

Social Engineering

The Objective?

They want to plant CDs or USB devices in conference rooms, bathrooms, and common areas of your facility.



The Goal:

- That one of you will find these devices and put the device in your computer.
- Once the device is used by an employee, it may try a download of customers' information or start a malicious attack on the network.

Security Best Practices

Social Engineering

The Objective?

They want to connect to the network or an unsecured computer.

The Goal:

- To perform scanning and/or hacking activities.
- To download a remote access program.
- To send confidential files over the Internet.
- To place a wireless access point on the network.



Security Best Practices

Social Engineering



Some of these objectives may sound pretty technical to you. To put it bluntly, if a social engineer gains access to your network, they have the potential of gaining the “keys to the kingdom”.

They can do anything they want with your systems and your business and customer information.

Security Best Practices

Social Engineering

Sec U R I T y

As you go about your work, be watchful for individuals that are behaving in a manner such as:

- Overly confident
- Overly friendly and talkative to you
- Telling you they forgot their swipe card or key fob
- Following close behind you as you enter the facility

Security Best Practices

Social Engineering

Sec U R I T y

- Posing as a vendor (heating & cooling technician, computer or printer technician)
- Posing as someone with law enforcement
- Posing as an auditor or examiner
- Showing you a business card and dropping names of South Dakota Housing Authority employees

Security Best Practices

Culture of Security

Core Value:

TEAMWORK...Supporting one another as we strive to create an exceptional working environment.



Security Best Practices

Phishing

From: jeffs@bhf-cu.net
Sent: Tuesday, October 21, 2014 3:04 PM
To: mark@sdhda.org
Subject: Mandatory Lender Training
Attached:  [Q4 Lenders.pdf \(40 KB\)](#)

Mark, We've hired new loan officers that require the mandatory SDHDA le
Attached is the list of new lenders. Can you please review the list and for
Thank you for your assistance.

Jeff Stephanoff
jeffs@bhf-cu.net
VP Business & Mortgage Lending
225 Main Street
Rapid City, SD 57709
605.718.1818
www.fhfcu.com



eral Credit Union's participating conditions in the First-time Homebuyer Program.
as well as Brenda Atkins?



Security Best Practices Phishing

From: vona@shda.org

Sent: Friday, October 31, 2014 4:30 PM

To: mark@sdhda.org; joni@sdhda.org; todd@sdhda.org; travis@sdhda.org; dalbrent@sdhda.org; gloria@sdhda.org; eileen@sdhda.org; ben@sdhda.org; moncarla@sdhda.org; lindsay@sdhda.org; tasha@sdhda.org; kris@sdhda.org; melolorraine@sdhda.org; denise@sdhda.org; lisab@sdhda.org; chas@sdhda.org; stacy@sdhda.org; doug@sdhda.org; laura@sdhda.org; pauls@sdhda.org; cristi@sdhda.org; barbara@sdhda.org; lee@sdhda.org; julie@sdhda.org; jill@sdhda.org; kenda@sdhda.org; jacque@sdhda.org; wayne@sdhda.org; beth@sdhda.org; slade@sdhda.org; amanda@sdhda.org; sheila@sdhda.org; mike@sdhda.org; stevem@sdhda.org

Subject: SDHDA Annual Conference

This year's annual conference was a huge success!

If you were unable to attend Patti Broer's breakout session on protecting information

[Protecting a Better Quality of Life](#)

Vona Johnson, Director

Rental Housing Management

South Dakota Housing Development Authority

PO Box 1237 :: 3060 East Elizabeth :: Pierre, SD 57501-1237

605.773.4567;; fax 605.773.5154

vona@sdhda.org;; www.sdhda.org

Building a Better Quality of Life



stacy@sdhda.org; doug@sdhda.org; laura@sdhda.org; pauls@sdhda.org; cristi@sdhda.org; barbara@sdhda.org; lee@sdhda.org; julie@sdhda.org; jill@sdhda.org; kenda@sdhda.org; jacque@sdhda.org; wayne@sdhda.org; beth@sdhda.org; slade@sdhda.org; amanda@sdhda.org; sheila@sdhda.org; mike@sdhda.org; stevem@sdhda.org

doubts in this email.

Security Best Practices

Phishing

From: doug@shda.org

Sent: Friday, October 31, 2014 4:30 PM

To: mark@sdhda.org; joni@sdhda.org; todd@sdhda.org; daleen@sdhda.org; jo@sdhda.org; eileen@sdhda.org; ben@sdhda.org; mona@sdhda.org; julies@sdhda.org; mary@sdhda.org; tasha@sdhda.org; kris@sdhda.org; melody@sdhda.org; kelly@sdhda.org; kevin@sdhda.org; lisab@sdhda.org; chas@sdhda.org; stephanie@sdhda.org; scott@sdhda.org; slar@sdhda.org

Cc: travis@sdhda.org

Subject: IMPORTANT Microsoft Lync Security Update!

Everyone, we've determined there's a zero-day threat within the Microsoft Lync

Please click on the link in this email to install the security patch. You'll be asked to provide information to verify your identity. Once you provide this information, the patch will complete its installation and your computer will be secure. It should take less than a minute for this process. Thank you for your

[Security Patch](#)

Doug Mahowald, Network Administrator
Network Administration

South Dakota Housing Development Authority
PO Box 1237 :: 3060 East Elizabeth :: Pierre, SD 57501-1237
605.773.4567 :: fax 605.773.5154
doug@sdhda.org :: www.sdhda.org

Building a Better Quality of Life



ra@sdhda.org; pauls@sdhda.org; cristi@sdhda.org; brent@sdhda.org; gloria@sdhda.org; jo@sdhda.org; julie@sdhda.org; jill@sdhda.org; carla@sdhda.org; lindsay@sdhda.org; wayne@sdhda.org; beth@sdhda.org; lorraine@sdhda.org; denise@sdhda.org; eila@sdhda.org; mike@sdhda.org; stevem@sdhda.org

...e don't install a patch on all computer systems.

...nce you provide this information, the patch will complete its installation and your computer will

Security Best Practices

Consumer Federation Phishing Video



A YouTube video player interface. The video frame shows a man in a dark suit and red tie, smiling and holding a document and glasses. The video title is "CFA Visa Phishing Scam". The video player controls show a progress bar at 0:04 / 2:37. Below the video, the channel name is "ConsumerFederation's channel" with a "Subscribe" button and a subscriber count of 65. The video view count is 4,105.



Security Best Practices

Core Value:

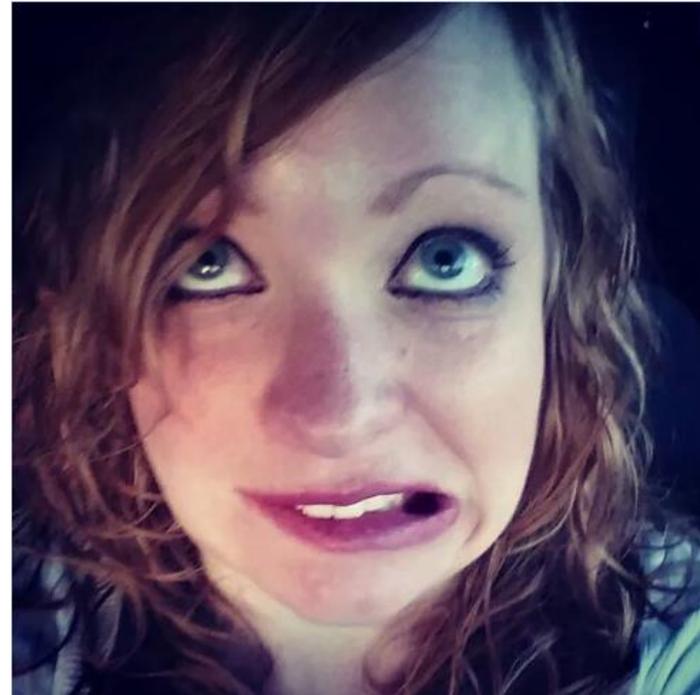
INNOVATION...Creating, embracing and accepting change for the betterment of the whole.

Security Best Practices

Social Media

What's posted on the Internet is out there for everyone to see.

It's a social engineer's dream!



Security Best Practices

Social Media

I ran my 10 miles today, Ugh!

Try this great casserole!

My guy is the greatest!

FORD outperforms Chevy every time!

I feel a migraine coming on, Ugh!

Security Best Practices Social Media

Amazing mind reader
reveals his 'gift'



Amazing mind reader reveals his 'gift'

Security Best Practices

October is Cybersecurity Awareness Month

The screenshot shows the FTC's website for Privacy & Identity. The header includes 'FEDERAL TRADE COMMISSION' and 'ESPAÑOL'. A search bar is present. The main content area is titled 'Privacy & Identity' and includes a sub-header 'Vea esta página en español'. Below this, there is a paragraph about the value of personal information. A prominent graphic for 'KIDS & computer security' features cartoon children. To the right, a 'Related Items' section lists links like 'Immediate Steps to Repair Identity Theft' and 'Credit Freeze FAQs'. A 'Recent Blog Posts' section lists articles such as 'Be smart about your phone' and 'A Bitcoin breakdown'. A left sidebar contains navigation links for various topics like 'MONEY & CREDIT', 'HOMES & MORTGAGES', 'HEALTH & FITNESS', 'JOBS & MAKING MONEY', 'PRIVACY & IDENTITY', 'BLOG', 'VIDEO & MEDIA', and 'SCAM ALERTS'.

FEDERAL TRADE COMMISSION ESPAÑOL

CONSUMER INFORMATION Search

MONEY & CREDIT

HOMES & MORTGAGES

HEALTH & FITNESS

JOBS & MAKING MONEY

PRIVACY & IDENTITY

Limiting Unwanted Calls and Emails

Computer Security

Kids' Online Safety

Protecting Your Identity

Repairing Identity Theft

BLOG

VIDEO & MEDIA

SCAM ALERTS

Privacy & Identity

Vea esta página en español

Your personal information is a valuable commodity. It's not only the key to your financial identity, but also to your online identity. Knowing how to protect your information — and your identity — is a must in the 21st century. Here are some tips to doing it effectively.

KIDS & computer security

Limiting Unwanted Calls & Emails

Some phone calls and emails are important, some can be annoying, and others are just plain illegal. Learn how to reduce the number of unwanted messages you get by phone and online.

Computer Security

The internet offers access to a world of products and services, entertainment and information. At the same time, it creates opportunities for scammers, hackers, and identity thieves. Learn how to protect your computer, your information, and your online files.

Kids' Online Safety

The opportunities kids have to socialize online come with benefits and risks. Adults can help reduce the risks by talking to kids about making safe and responsible decisions.

Protecting Your Identity

Keeping your important papers secure, shredding documents with sensitive information before you put them in the trash, and limiting the personal information you carry with you are among the ways you can protect your identity. Find additional tips to reduce your risk of identity theft, including how and when to order your free credit report.

Repairing Identity Theft

If you suspect someone has stolen your identity, acting quickly to limit the damage is key. Take a deep breath, and then place a fraud alert on your credit file, order your credit reports, and call the FTC to report the crime.

Related Items

What is Identity Theft?

- Immediate Steps to Repair Identity Theft
- Credit Freeze FAQs
- How to Keep Your Personal Information Secure
- Spam
- Kids and Socializing Online

Recent Blog Posts

- Be smart about your phone October 3, 2014
- A Bitcoin breakdown September 23, 2014
- Staying current: Bitcoin and other cryptocurrencies September 23, 2014

<http://www.consumer.ftc.gov/topics/privacy-identity>

Security Best Practices

October is Cybersecurity Awareness Month

[Welcome | Stop Think Connect](#)

The screenshot shows the homepage of the Stop Think Connect website. At the top, there is a navigation bar with the logo 'STOP | THINK | CONNECT' and the tagline 'Keeping the web a safer place for everyone.' To the right, there is a 'Partner Resource Center Login' section with input fields for 'email' and 'password', and a 'Forgot Password?' link. Below the navigation bar, there is a horizontal menu with buttons for 'HOME', 'RESOURCES', 'CAMPAIGNS', 'GET INVOLVED', 'TIPS & ADVICE', 'RESEARCH & SURVEYS', 'BLOGS', and 'ABOUT US'. The main content area features a large banner with a photo of three people (a man, a woman, and an older woman) looking at a laptop. Overlaid on the banner is the text 'DO YOUR PART TO MAKE THE INTERNET SAFER FOR EVERYONE.' To the right of the banner is a 'TWO STEPS AHEAD' section with a padlock icon and the text 'PROTECT YOUR DIGITAL LIFE' and 'Protect your digital life by adding layers of security to your online accounts.' Below this is a 'LEARN HOW' button. At the bottom left, there is a 'STOP. THINK. CONNECT.' section with a green circular graphic containing white dots and the word 'October'. To the right of this is a 'DID YOU KNOW?' section with the text '61% of Americans believe that much of online safety falls under their personal control.' To the right of that is a 'Get Involved!' section with icons for a smartphone, a tablet, and a laptop, and the text 'It's easy to get involved with STOP. THINK. CONNECT. We're creating free resources for anyone to use.' Below this is a 'GET STARTED' button.

Security Best Practices

Core Value:

PROFESSIONALISM...Displaying leadership, excellence, respect, empathy and open-mindedness in EVERYTHING we do.

Security Best Practices

Our Core Values

PROFESSIONALISM...Displaying leadership, **excellence**, **respect**, empathy and open-mindedness in everything we do.

INTEGRITY...Being **honest** and **ethical**.

ACCOUNTABILITY...**Taking responsibility for our actions** and following through in a consistent, reliable and timely manner.

INNOVATION...Creating, embracing and **accepting change** for the betterment of the whole.

COMMUNICATION...**Sharing information**, ideas and opinions with clarity and understanding, **ever mindful of respecting confidentiality**.

TEAMWORK...Supporting one another as we strive to create an exceptional working environment.



Security Awareness

YOU are the First Line of Defense



Protecting a Better Quality of Life

- ❑ Security Awareness
- ❑ Information Security Mindset
 - ❑ Needs to become SECOND NATURE
 - ❑ Needs to be the HEARTBEAT of your job
- ❑ Security Best Practices



Whatever it Takes

The poet William Arthur Ward said:

1. "I will do more than belong—I will participate.
2. I will do more than care—I will help.
3. I will do more than believe—I will practice.
4. I will do more than be fair—I will be kind.
5. I will do more than forgive—I will forget.
6. I will do more than dream—I will work.
7. I will do more than teach—I will inspire.
8. I will do more than learn—I will enrich.
9. I will do more than give—I will serve.
10. I will do more than live—I will grow.
11. I will do more than suffer—I will triumph."

You can't do whatever's easiest and still reach your goal.

You must do more.

You must do "whatever it takes."



Resources

- ❖ informationisbeautiful.net
- ❖ aba.com/protectyourmoney
- ❖ NIST (National Institute of Standards and Technology U.S. Department of Commerce Special Publication 800-50)
- ❖ NISTIR 7621 Small Business Information Security: The Fundamentals
- ❖ South Dakota Attorney General - atg.sd.gov
- ❖ Secure Banking Solutions, LLC www.protectmybank.com
- ❖ Wikipedia
- ❖ www.consumerfed.org/fraud
- ❖ www.idtheftinfo.org
- ❖ www.onguardonline.gov
- ❖ www.youtube.com
- ❖ <http://www.stopthinkconnect.org/>
- ❖ <http://www.consumer.ftc.gov/topics/privacy-identity>

Patti Broer, Information Security Administrator and Business Continuity Plan Coordinator, BankWest Inc.:

- *Supports and assists with the \$800 million South Dakota-based bank's incident response plan, as it relates to breaches of information security.*
- *Supports and assists with the bank's information security program, which includes privacy, social engineering and security awareness training for employees, security oversight and administration of most of the bank's software applications as well as supporting and assisting with BankWest's vendor management program.*
- *Maintains BankWest's business continuity plan by coordinating annual updates and conducting enterprise-wide table-top exercises.*
- *Serves on the Board of Advisors for BankInfoSecurity.com and has been employed at BankWest for 28 years.*

