Computer Security for Business and Home: Best Practices

Orcas Island Chamber of Commerce

Tony P. Ghazel, 5 May 2010

What we will be discussing!

- Top five things you can do (Quick Discussion)
- Security best practices
- Securing your business or home network
- Online Banking

Top five things you can do for safe computing

1. Use security software
2. Practice the principle of least privilege
3. Maintain current software and updates
4. Physically secure your computer
5. Firewall

Use security software

- The most important thing you can do to keep your computer safe is to install and maintain security software, which protects your computer from viruses and spyware. Such security programs perform two general functions: scanning for and removing viruses and spyware in files on disks, and monitoring the operation of your computer for virus-like activity.

- **Use Anti-Virus Software**

  Anti-Virus software is used to protect your computer against malicious software (or Malware).

  You may already be using anti-virus software but to be effective the following should be followed:

  - The Anti-Virus software should be updated on a regular basis with the latest virus definition files.
  - The Anti-Virus software should always be running and providing real time protection on your desktop computer, especially when connected to the internet.

  There are many Anti-Virus software to choose from some are commercial and others that are free, below is a list of the most common anti-virus products:

  Some commercial products include:

  - AVG Anti-Virus
  - BitDefender
  - CA eTrust Integrated Threat Management
  - E Scan
  - F-Prot
  - F-Secure
  - Kaspersky Anti-Virus
  - LinuxShield
  - McAfee VirusScan
  - Norton AntiVirus
  - Panda Antivirus
  - PC-cillin
  - Windows Live OneCare
  - ZoneAlarm AntiVirus

  Some freeware products include:

  - AOL Active Virus Shield
  - AVG Anti-Virus Free
  - avast! Home
  - Comodo AntiVirus

- **Antivirus Software 2010:** Trend Micro antivirus with anti-spyware protects PCs from spyware, anti-phishing, virus, trojans and all other Internet threats. Best of all, it keeps intruders out and sensitive information in with a two-way firewall.
- **Firewall - ZoneAlarm Pro:** The best way to secure your private information on your PC. Free services help you discover and recover from identity theft. ZoneAlarm Pro provides you with firewall with privacy protection. Scans for and removes thousands of spyware
- **AVG Antivirus with Anti-Spyware:** AVG 8.5 brings a complete level of computer protection against the newest threats. It includes antivirus, firewall, with anti-spyware, and anti-spam. On top of that, the last major feature is a free support and
- **PC Tools Internet Security 2010:** is advanced technology designed especially for people, not just experts. It is automatically configured out of the box to give optimal protection with limited interaction. Best of all, it allows you to control
- **Norton 360 - Premier Edition:** This new version detects and stops viruses, spyware, rootkits and other hidden threats automatically at their entry point or quarantines infected files when one is found on your computer. Protects up to 3 PCs per household.
- **ESET Smart Security 4:** Based on ESET NOD32 Antivirus, it protects you from viruses, worms, spyware, and all Internet threats; also blocks spam and includes personal firewall. Named "Consumer Digest Best Buy" in April 2008.
- **CensorNet Web Filter:** CensorNet is a software solution for Web Content Security that protects against undesirable web sites and web based threats, delivering enhanced security and compliance.
- **Free Spyware Remover:** Most computers that are connected to the internet today are infected by some sort of adware and spyware. You may have invested in the best security tools, but still it is advisable to use…
- **Free PC Optimize Scan:** CA Anti-Spam software provides spam protection for multiple POP3 email account. Another great feature of this software is that it will be able to help in preventing phishing attacks. Easy-to-use, no brainer.
- **Security Scanner for Home Users:** Infiltrator can audit each scanned computer for improper registry settings, suspicious open ports, vulnerable services, scripting exploits, weak password policies, and improper user configurations The program can be
- **GFI Software:** Leading developer of network security, content security and messaging software. Its product range includes email content exploit checking and anti-virus software; security scanning and patch management tools.
- **Bloxx Tru-View Technology** : Bloxx Web filtering performs live analysis and real time categorization of Web pages at the point of user request, giving you fuller coverage of the Internet and dramatically improving protection and security. Radically different from other web filters.
- **Registry Mechanic:** This registry cleaner allows you to repair and optimize the Windows registry. The program is able to remove orphaned references which can significantly improve your system's stability. Free customer support for all users.

- **Use an anti-spyware program**

Spyware is the term used to describe programs that run on your computer for the purpose of monitoring and recording the way in which you browse the web and the internet sites you visit. In addition spyware can be used to extract personal information that you have entered, including passwords, telephone numbers, credit card numbers and identity card numbers.
Spyware is often loaded onto a PC as part of a free download of another service. Sometimes your agreement to the download is requested in the small print, but spyware may also be loaded onto your PC without your agreement or knowledge through websites that you visit over the internet.
Spyware is not the same as a virus in that it only records what you do rather than altering how your machine works. Because of this, anti-virus software is not effective in identifying and removing spyware; you will need to download and run a specialized anti-spyware program.

Some Anti-spyware security software include:

- McAfee AntiSpyware.
- Spybot Search and Destroy.
- Spyware Eliminator.
- Spyware Doctor.
- Microsoft antispyware.

We strongly recommend that you install and use a reputable anti-spyware product to protect yourself against spyware on your PC.

Practice the principle of least privilege (PoLP)

- Practice the principle of least privilege. Do not enable administrative privileges until needed; in other words, do not log into a computer with administrative rights unless you must do so in order to perform specific tasks. Running your computer as an administrator (or as a Power User in Windows) leaves your computer vulnerable to security risks and exploits. Simply visiting an unfamiliar Internet site with these high-privilege accounts can cause extreme damage to your computer, such as reformatting your hard drive, deleting all your files, and creating a new user account with administrative access.

- **Protect your passwords follow best practices**

a- Avoid using the same password for different accounts, because if the password is found by an unauthorized person all your accounts
will be at risk.

b- Use strong passwords, Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

c- Never write passwords down. If, however, you feel that you have no alternative but to do so, you should ensure to write down your
passwords in a way that cannot be understood by somebody else and lock them in a secured location.

d- In any event, you should never disclose your Internet login details anywhere online except at your usual known and used websites, which
should be accessed in the normal way and never via a link in an email.

e- Always change your password whenever you think it is compromised in anyway.

Maintain current software and updates

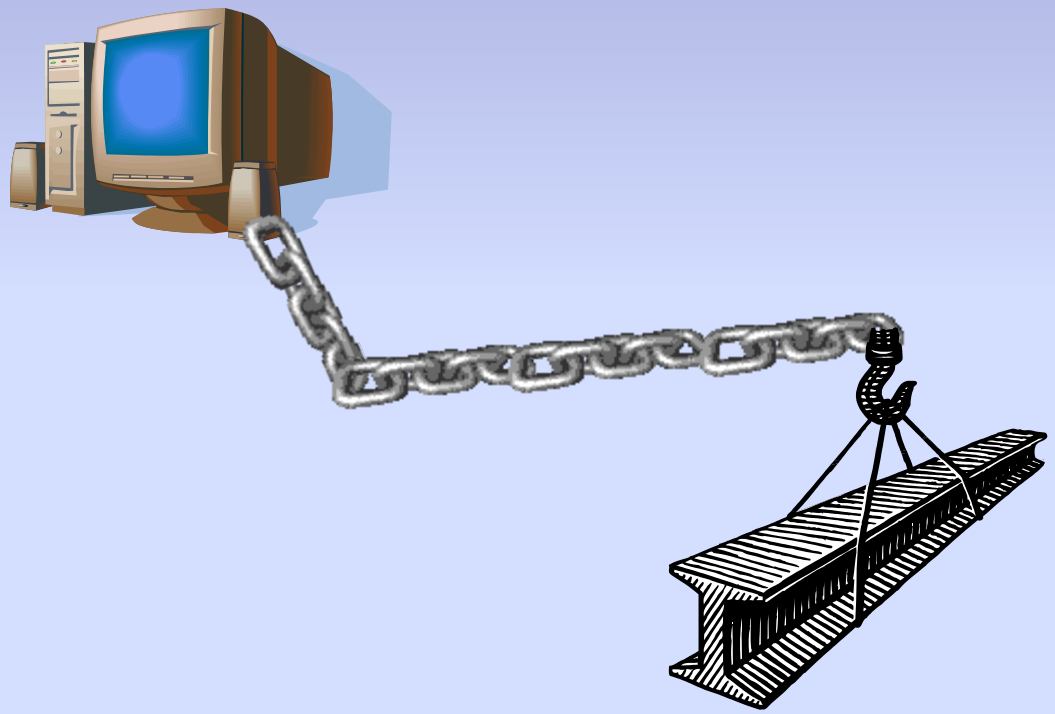
- Keep your software updated by applying the latest service packs and patches. For Windows, you can schedule Automatic Updates to automatically download and install available updates.

- **Update your system with the latest security updates & patches**

  Security updates and patches are used to fix vulnerabilities (or weaknesses) that are discovered in programs, applications or the host operating system (ex: windows 2000\XP\ Vista or any Linux distribution etc…) running on your PC. These patches are published by your software vendor, always be sure to install these updates and always be sure that you are getting them from your trusted vendor site or resource.
  If your systems are not updated, virus writers and hackers can use the vulnerabilities on your system to gain unauthorized access to your PC.

  N.B. Microsoft users can visit: http://windowsupdate.microsoft.com to update their systems.

Physically Secure Your Computer



Firewall

- What is a firewall
  - A **firewall** is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices which is configured to permit or deny computer based application upon a set of rules and other criteria. (wikipedia)
- How does it work?
- Do I need one?

- **Use personal firewalls**

  A personal firewall is a small program that helps protect your computer and its contents from outsiders and hackers on the Internet.
  When installed, it stops unauthorized traffic to and from your PC as well as blocking un-safe websites and logging internet activity.

  You can choose from several personal firewalls some common ones are mentioned below:

  - Zone Labs (ZoneAlarm)
  - McAfee (VirusScan Plus)
  - F-Secure (F-Secure Internet Security)
  - Computer Associates (CA Personal Firewall 2007).
  - Internet Security Systems (BlackICE PC Protection).
  - Freeware (Comodo Personal Firewall).
  - Microsoft (free Windows Firewall built into Windows XP-SP2 and Vista).

Security Best Practices

1. Never share passwords or passphrases
2. Do not click random links
3. Beware of unknown email and attachments
4. Don't download unknown software off the Internet
5. Don't propagate hoaxes or chain mail
6. Log out/lock your computer
7. Shut down computers
8. Remove unnecessary programs
9. Restrict remote access
10. Frequently back up important files
11. Treat sensitive data carefully
12. Remove data securely
13. Deploy encryption when possible

1. Never share passwords or passphrases (Review)
   - Pick strong passwords and passphrases, and keep them private. Never share your passwords or passphrases, even with friends, family, or computer support personnel.
2. Do not click random links
   - Do not click any link that you can't verify. To avoid viruses spread via email or instant messaging (IM), think before you click; if you receive a message out of the blue, with nothing more than a link and/or general text, do not click it.

3. Beware of unknown email and attachments
   - from unknown people, or with a strange subject line

信用狀到期還單代償。現金貸款。合法租賃公司'客票貼現'年息17%。房屋全額貸款。服務電話：０９５８５６９０３５·押標金銀行代墊款手續費1%。Wed, 21 Apr 2010 16:02:01 +0200 ✆ to tg.global

show details 6:57 AM (0 minutes ago)

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more

Chinese (Traditional Han)> English Translate messageTurn off for: Chinese (Traditional Han)

誠信經營。房屋全額貸款。服務電話：０９５８５６９０３５·凡已向銀行貸款者，或未貸款者。L/C額度申請。Wed, 21 Apr 2010 17:02:01 +0300

合法租賃公司'客票貼現'年息17%

房屋全額貸款

二胎房貸'中古車貸款

增資驗資，存款證明

訂單貸款

銀行換單代墊

各式珠寶'鑽石'名錶'

租賃基本架構

機械設備租賃與分期

大型船舶各種租賃與分期

航空器、飛機引擎各種租賃與分期

海外台商融資租賃分期

專案業務租賃與分期(Project Finance)

廠辦、商辦售後租回

土地整合/合作開發

歡迎您來電:０９５８５６９０３５

·營運週轉金。買屋不用頭款。專辦農地。空地。道路地。公司工廠。貸款。Wed, 21 Apr 2010 07:56:01 -0600

Year 2010 Mad Sale, Rep1icaWatches only from $196:- BvlgariRolexDior, Cartier, Audemars Piguet, Oris, Panerai, Ebel & brand new models vztv t75

SpamX

Reply | Jena Jose ✆ to lynnstone, bcc: juan05, bcc: alcongo, bcc: rbw185, bcc: 7nationarmy, bcc: jdhalter, bcc: me, bcc: prman01, bcc: keminmem

show details Apr 11 (4 days ago)

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more

** The Best & Finest Rep1icaStore on net

** The cheapest among all other online Rep1icaSites

** over 40 world famous brandedWATCHES BRANDs to choose from

http://platefrease.com

* oRolexDatejusts

* oRolexSports

* A Lange & Sohne

* Aigner

* Alain Silberstein

* Audemars Piguet

* Breitling

* Bvlgari

* Bell & Ross

* Breguet

* Cartier

- 1986 Mercedes-Benz 560SEL with 80,000 miles and Car Cover - $2000 (Orcas Island, Washington)

From: Nihet Kaine (nihetkcemew@hotmail.com)

Sent:Sun 4/25/10 11:53 AM

To: ♍♒❒♓♦♑♒♋⌘♏●@hotmail.com

- First of all, go here: http://we-hire.webs.com/ We are starting people off at $1000-$2000 per week Hi, I saw your cars & trucks - by owner ad and I simply felt like saying hello. Is it still for sale? It's funny, my husband is very much into these kinds of things althought I can't claim I care for them too much . I'll forward the ad to him, see if he wants to pick it up. Let me get to the point and keep this short. Since you're trying to sell on Craigslist, you are probably trying to generate a little bit of extra income. This is NOT an ad, I am not selling you ANY products, EVER. I work for SMC and we are always looking for people that know their way around the web, etc... We pay roughly $1000 to $2000/week. I will talk to my boss and see if we can't setup an interview and get you started this Wednesday as a part time job. You'll be earning from your home. Please contact me here: http://we-hire.webs.com/

From: Joyce ♆♋♦♦♦ <jaw1436@yahoo.com>

Date: Fri, Apr 30, 2010 at 7:38 AM

Subject: in need of your help

To: jaw1436@yahoo.com

I hope you receive this message on time ? Sorry I didn't inform you about my trip to the Scotland for a program,I am presently in Scotland, something extremely dreadful happened to me,I was rubbed at gun point on my way to the Hotel by by hooligans and they made away with my Bag and other valuables. I called my bank for a wire transfer but it has proven almost Impossible to operate my account from here as they made me understand international transactions take 7 working days to be effective which i can't wait.

I feel so devastated,now my passport and other belongings are been retained by the hotel management pending the time I pay my Hotel bills.This is shameful,I need you to help me with a loan of 1600 pounds (equivelent to $2500) to pay my hotel bills and get my self home.I will reimburse you soon as I get back Home.I will appreciate whatever you can assist me with. Let me know if you can be of help.

All hopes on you.

joyce

- Nigerian Scam
- Banking Scams
- Facebook
- Recheck your email passswords
- Ebay verify your account
- Your grandson needs money
- Etc

4. Don't download unknown software off the Internet
   - KaZaA, Bonzi, Gator, HotBar, WhenUSave, CommentCursor, WebHancer, LimeWire, etc, all appear to have useful and legitimate functions. However, most of this software is or contains spyware, which will damage your operating system installation, waste resources, generate pop-up ads, and report your personal information back to the company that provides the software.

5. Don't propagate hoaxes or chain mail
   - No More Said!
   - Check it out at www.snopes.com
6. Log out/lock your computer
   - Forgetting to log out poses a security risk with any computer that is accessible to other people (including computers in public facilities, offices, and shared housing) because it leaves your account open to abuse. Someone could sit down at that computer and continue working from your account, doing damage to your files, retrieving personal information, or using your account to perform malicious actions. To avoid misuse by others, remember to log out of or lock your computer whenever you leave it.

7. Shut down computers

   I normally recommend to leave computers on while away; but, make sure that you are logged off.

8. Remove unnecessary programs

9. Restrict remote access
   - Remote access, File sharing etc by default are not very secure.
10. Frequently back up important files
   - This protects your data in the event of an operating system crash, hardware failure, or virus attack. I recommend saving files in multiple places using two different forms of media (e.g., USB flash drive, CD-R). And, on a rotating basis.
11. Treat sensitive data carefully
   - For example, when creating files, avoid keying the files to Social Security numbers

12. Remove data securely
    - Remove files or data you no longer need to prevent unauthorized access to them. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system.
    - dban.org, east-tec.com, heidi.ie/eraser and others
13. Deploy encryption when possible
    - See a specialist

Banking Online

- How does my online banking session take place?
- What are the basic security risks of Internet communications?
- How does security technology protect against these risks?
- To what degree can SSL security protect me?
- How do my bank's online security measures protect me?
- What is encryption?
- Phishing attacks

How does my online banking session take place?

- An online banking session is started when the authorized subscriber uses his or her browser to send a secure message via SSL to your financial institution's (bank's) server. For this purpose he uses the customized password, along with his User ID. The server verifies this data and responds by authenticating the customer and initiating session encryption.
- Once your session is securely established, the server processes and routes the transaction data using internal protocols. This prevents other Internet users from proceeding past the bank's series of firewalls and filtering routers.
- Robust bank's online servers protect financial transactions through a number of barriers that prevent unauthorized access. The first barrier is a system of filtering routers and firewalls, which separates the outside Internet from the institution's internal network. The filtering router verifies the source and destination of each Internet packet, and determines whether or not to allow the packet through. Access is denied if the packet is not directed at a specific available service. In addition, the filtering router prevents many common Internet attacks.
- Furthermore, a good firewalling scheme, which many financial institutions utilize, will not allow servers in the bank's network to communicate via TCP/IP - the Internet communication protocol. No internal online transaction processing systems are reachable using TCP/IP. This prevents unauthorized users from accessing any transaction data from the Internet.
- The information is passed between the bank's main server and the customer's PC after it is duly encrypted using the highest possible encryption.

What are the basic security risks of Internet communications?

- Sending data across a network involves three basic security risks:

  Eavesdropping - intermediaries listen in on private conversations (one computer talking to another).
  Manipulation - intermediaries change information in a private communication.
  Impersonation - a sender or receiver communicates under false identification.

  The situation is analogous to purchasing mail-order goods over the telephone. Mail-order shoppers want to know that no third party can hear their credit card number (eavesdropping); that no one can insert extra order information, or change the delivery address (manipulation); and that it is actually the mail-order company on the other end of the line and not a credit card thief (impersonation).

How does security technology protect against these risks?

- Current browsers counter security threats with a network communication protocol called Secure Sockets Layer (SSL). SSL is a set of rules that tells computers the steps to take to improve the security level of communications. These rules are designed for the following:

  - Encryption, which guards against eavesdropping.
  - Data integrity, which guards against manipulation.
  - Authentication, which guards against impersonation.

  However, these effects protect your data only during transmission. That is, network security protocols do not protect your data before you send it. Just as you trust merchants not to share your credit card information, you must trust the recipients of your online data not to mishandle it.

To what degree can SSL security protect me?

- SSL uses authentication and encryption technology developed by RSA Data Security Inc. The encryption established between you and a server remains valid over multiple connections, yet the effort expended to defeat the encryption of one message cannot be leveraged to defeat the next message.

  A message encrypted with 40-bit RC4 takes on average 64 MIPS-years to break (a 64-MIPS computer needs a year of dedicated processor time to break the message's encryption). The high-grade, 128-bit U.S. domestic version provides protection exponentially more vast. The effort required to break any given exchange of information is a formidable deterrent. Server authentication uses RSA public key cryptography in conjunction with ISO X.509 digital certificates.

How do my bank's online security measures protect me?

- Banks should be committed to providing the safest Internet banking service to their customers so that all transactions involving financial and customer data are conducted in a safe and secure environment. Without thorough security, information transmitted over the Internet is susceptible to fraud and other misuse by intermediaries. Information traveling between your computer and a server uses a routing process that can extend over many computer systems. Any of these computer systems represents an intermediary with the potential to access the flow of information between your computer and a trusted server. You need security to make sure that intermediaries cannot deceive you, eavesdrop on you, copy from you, or damage your communications.

  Adequate security features are in-built into reputable banks online services to protect customers. Most banks use 128-bit encryption, the highest encryption security currently available, which was earlier restricted to Canada and the U.S.A., but are now available to Banks outside the U.S.A. Additional security comes with the User ID and Password, which are provided to you by the bank to access your account. The information, which you enter, passes through 128-bit encryption.

  Microsoft Internet Explorer with 128-bit encryption uses:
  - Server authentication (thwarting impostors).
  - Privacy using encryption (thwarting eavesdroppers).
  - Data integrity (thwarting vandals).
  - Firewall is used to protect data in a bank's main computer and only authorized persons have appropriate access to the data in the system.
  - The SSL protocol delivers server authentication, data encryption, and message integrity. SSL is layered beneath application protocols, such as, HTTP, SMTP, Telnet, FTP, Gopher, and NNTP, and layered above the connection protocol TCP/IP. This strategy allows SSL to operate independently of the Internet application protocols.
  - With SSL implemented on both the client and server, your Internet communications are transmitted in encrypted form. Information you send can be trusted to arrive privately and unaltered to the server you specify (and no other).

- Customer information and account data is protected by two independent security protocols: data encryption and a verifiable Password. When bank customers use online banking, they are first prompted to enter their Password. The receiving computer will not send any account information to the customer's computer unless the Password associated with the User ID has been correctly entered. All information that passes between the bank's servers and the customer's computer is put through data encryption.

- A bank's success as a financial institution depends on its ability to manage these systems safely and to continue to earn your trust as a customer. By requiring 128-bit encryption, a bank is assuring the highest level of commercially available security for your financial transactions.

What is encryption?

- Encryption is the scrambling of information for transmission back and forth between two points.
  When you send out a letter to your friend, you communicate in a language that both of you understand. Since your language is also understood by thousands of other people, if someone else should get hold of your letter, he will not have any problem in understanding its contents. If you do not want anyone other than the party to whom your letter is intended to understand your message, you must use a secret language or you must substitute each alphabet in your letter for some other alphabet, which only the two of you will understand. Using a secret language or substituting one alphabet or word for another is called encryption and your letter is said to be encoded. To decode your letter, the receiver must have the same key that you used for encoding. To any other person who does not have this key, the contents of your message will not make any sense and will be garbage.
  Computers also use the same principle. The browser in your computer uses a string of numbers, characters and special keys and makes the encoding and decoding immensely complicated. Your computer and the one at the receiving end agree upon the keys to be used for encoding. These keys are based on a set of mathematical formulae called algorithms. When a computer encrypts a message, there are billions of key combinations to select from. However, only one of the billions of combinations will be correct. Only the computers on both ends of the transaction know what key combination is in use during that session. The sending and the receiving computers use a different key combination for each session and only these two computers know what key is used for the current session. So if anyone else tries to read your message, he will only get meaningless string of numbers and characters.
- Encryption finds its application in a variety of transactions that involves sensitive matters and even for national security. Encryption is used for sending e-mail messages, sensitive documents and in electronic commerce, such as, credit card transactions and electronic banking.
- The security provided by encryption is measured in terms of the time frame the encoding key is used by your computer for encryption. The level of encryption is measured in bits like 40-bit or 128-bit encryption.
  If the encryption has a 40-bit key, it means that there are 240 possible different combinations for solving the key. Similarly, for a 128-bit key, there are 2128 possible different combinations. In general, the longer the key, the longer it would take for someone without the correct decoder key to break the code.
- The 40-bit encryption and the 128-bit encryption differ in their complexity and the key length. 40-bit encryption can use one of the 240 possible different combinations (1 followed by 12 zeroes) and 128-bit encryption uses one of the 2128 possible different combinations (3.4 followed by 38 zeroes). 128-bit encryption is exponentially more powerful than 40-bit encryption.
- 40-bit encryption is not as powerful as 128-bit encryption, but this still requires a great deal of dedicated effort to break. When the length of the key is increased by one bit, the amount of effort required for breaking the code doubles. However, as the power in the hands of the potential criminals increases, it is necessary to use a more complex and longer key for secure transmission of data electronically. This is being provided by 128-bit encryption.
  According to Netscape, 128-bit encryption is 309,485,009,821,345,068,724,781,056 times more powerful than 40-bit encryption.
- For Microsoft browsers: You can find out the level of encryption by using your browser menu bar. Select "File" then "Properties" then "Security."
  When you visit a site that requires encryption, your browser will display the symbol with a key or a lock. If you are not in a secure area, the key or lock will be broken.
- Customer information and account data is protected by two independent security protocols: data encryption and a verifiable Password. When bank customers use online banking, they are first prompted to enter their Password. The receiving computer will not send any account information to the customer's computer unless the Password associated with the User ID has been correctly entered. All information that passes between the bank's servers and the customer's computer is put through data encryption.
- A bank's success as a financial institution depends on its ability to manage these systems safely and to continue to earn your trust as a customer. By requiring 128-bit encryption, a bank is assuring the highest level of commercially available security for your financial transactions.

Phishing attacks

- **What is Phishing?**

PHISHING: is an online identity theft technique used to lure customers into disclosing their personally identifiable information including account names and passwords, and credit card information. This technique is widely in use in the digital world, oftentimes customers are sent emails, pop-ups, and instant messages that mimic legitimate communications. These communications prompt the user to visit fraudulent websites created to gather their personal information. Financial institutions, banks and online retailers are most susceptible to having their communication spoofed in phishing attempts. In the end, costumers are lured in by these seemingly legitimate communications into providing sensitive information, often resulting in credit card fraud; identify theft, and even financial loss.

How to recognize a phish (fraudulent) email as not sent from my bank?

Your bank should not request personal information from customers directly from an email-hyperlink or redirect the customer to a specified site.
Your bank should never send emails asking customers to supply, verify, or update personal or account information. Especially requests pertaining to passwords, PIN's, and account numbers.
Your bank's emails should always be personalized emails identifying the sender of the email as a legitimate bank employee and identifying the receiver as the bank's customer. Sending emails with personalized information helps you identify legitimate versus spoofed emails.

Securing your business or home network

1. Local Area Network
   - Local Area Networks (LAN) are more secure since a friendly or unfriendly computer cannot communicate with other computers on the network without being "plugged" in
2. Wireless Network
   - A Wireless Network is inherintly insecure since someone could be in the parking lot and can have uninvited access to your network and other computers on the network.

Securing a Wireless Network

1. Disable SSID Broadcast
2. Change the default SSID
3. Use encryption for access:
   - WPA2/WPA (Wi-Fi Protection Access)
   - WEP (Wired Equivalency Privacy).
4. Enable strong passwords for your wireless router's admin page
5. Disable remote administration
6. MAC Address Filtering

UTILITIES

- Port Scanner
  - **LANguard Port Scanner 1.0 (lanportscan.exe)**
  - FTP 21
  - Telnet 23
  - SMTP 25
  - POP 110
  - Web Browsing 80, 8080
- DNS Tester
  - dnstoolbox.com
- Mail Server Query and Black List
  - mxtoolbox.com

Questions and Wrap-up

Thank You!