Securing Online Transactions

Module 8

Simplifying Security.

Certified Secure Computer User

Module 8: Securing Online Transactions

Exam 112-12

Module Objective

Online transactions help the consumers in purchasing products, paying bills, and more. It combines creative and technical features of the Internet with design, development, advertising, and sales using websites with effective content for a product or service. In contrast, **fraudsters** can take advantage of online transactions to gain access to the customers' confidential information.

This module will familiarize you with:

- Online Shopping
- How Online Shopping Works?
- Online Banking
- Securing Online Transactions
- Choosing a Secure Online Payment Service
- SSL and the Padlock Symbol
- Identifying a Trustworthy Website
- Identifying an Untrustworthy Website
- McAfee's Site Advisor
- Guidelines for Secure Online Transactions

Module Flow

Online Shopping

How Online Shopping Works

Online Banking

Securing Online Transactions

Choosing a Secure Online Payment Service

SSL and Padlock Symbol

Identifying a Trustworthy Website

Identifying an Untrustworthy Website

Online Transaction Security Checklist

Online Shopping

Online shopping is the process of buying goods and services over the Internet. Through online shopping, a consumer can **purchase** a variety of products such as clothes, household equipment's, books, toys, and more. Of late, there is an increasing tendency among global consumers to use online sites for shopping because it can be done at **any time** and from **anywhere**. Keeping in tune with this trend, retailers are promoting goods and services on websites and providing the option of buying products online. As a result, goods and services are now traded over the network through **www-based catalogs**. Consumers usually pay their bills by providing credit cards details, which are unencrypted. To secure the payments, banks have also introduced card-based payment schemes across the network. These payments are secured using cryptography techniques.

Benefits of online shopping include:

- Usually available 24 hours a day
- Describe products with text, photos, and multimedia files
- Quickly seek out deals for items/services with several vendors
- Purchase a product without actually traveling to the store using credit/debit card

How Online Shopping Works

The following steps describe how online shopping works:

- Go to any desired e-commerce site:

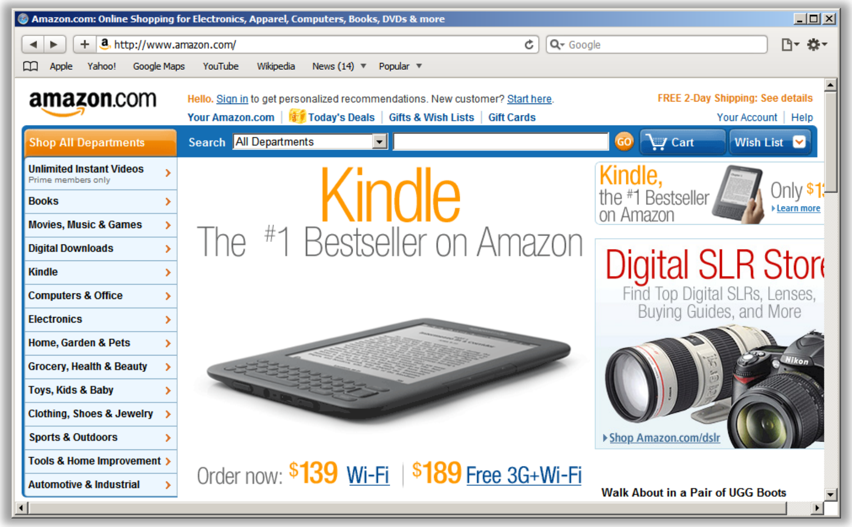
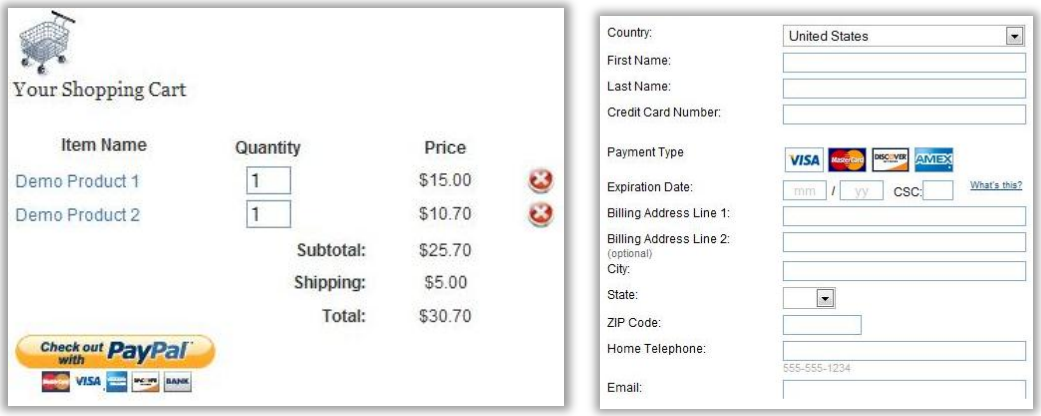


Figure 08-01: E-Commerce Site

- Browse for the required product through the online catalogue

- Add the product/service to the shopping cart. The shopping cart shows:
- The products being purchased
- The number of product units
- The price of the product and taxes (inclusive/exclusive)
- Shipping costs and more



Your Shopping Cart

Item Name	Quantity	Price
Demo Product 1	1	$15.00
Demo Product 2	1	$10.70
	Subtotal:	$25.70
	Shipping:	$5.00
	Total:	$30.70

Country: United States

First Name:

Last Name:

Credit Card Number:

Payment Type

Expiration Date: mm / yy CSC: What's this?

Billing Address Line 1:

Billing Address Line 2: (optional)

City:

State:

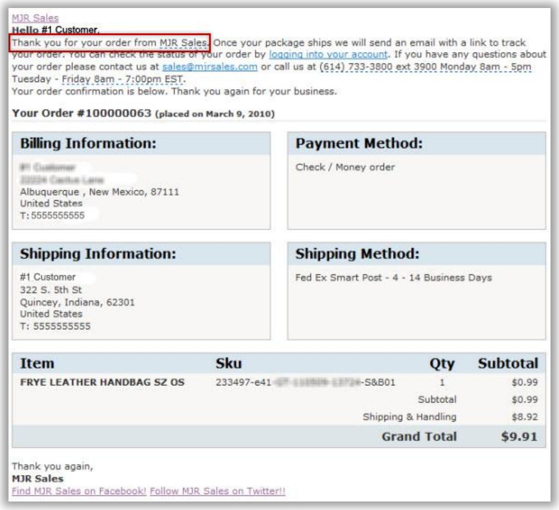
ZIP Code:

Home Telephone: 555-555-1234

Email:

Figure 08-02: Online Payment Screenshots

- Fill in the online order form with:
  - Shipping information
    - Shipping address
    - Consumer name
  - Billing details
    - Credit card details
    - Billing address
  - Any other information the merchant requires



MJR Sales

Hello #1 Customer,

Thank you for your order from MJR Sales. Once your package ships we will send an email with a link to track your order. You can check the status of your order by logging into your account. If you have any questions about your order please contact us at sales@mirsales.com or call us at (614) 733-3800 ext 3900 Monday 8am - 5pm Tuesday - Friday 8am - 7:00pm EST.
Your order confirmation is below. Thank you again for your business.

Your Order #100000063 (placed on March 9, 2010)

Billing Information:
[redacted]
Albuquerque , New Mexico, 87111
United States
T: 5555555555

Payment Method:
Check / Money order

Shipping Information:
#1 Customer
322 S. 5th St
Quincey, Indiana, 62301
United States
T: 5555555555

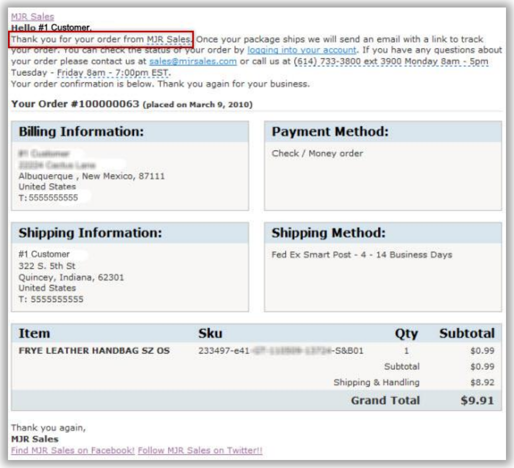
Shipping Method:
Fed Ex Smart Post - 4 - 14 Business Days

Item	Sku	Qty	Subtotal
FRYE LEATHER HANDBAG SZ OS	233497-e41[redacted]-S&B01	1	$0.99
		Subtotal	$0.99
		Shipping & Handling	$8.92
		Grand Total	**$9.91**

Thank you again,
MJR Sales
Find MJR Sales on Facebook! Follow MJR Sales on Twitter!!

Figure 08-03: Invoice Screenshot

- The credit card information is then encrypted and sent to the merchant.
- The customer receives an on-screen confirmation and/or a confirmation email.



MJR Sales
Hello #1 Customer,
Thank you for your order from MJR Sales. Once your package ships we will send an email with a link to track your order. You can check the status of your order by logging into your account. If you have any questions about your order please contact us at sales@mirsales.com or call us at (614) 733-3800 ext 3900 Monday 8am - 5pm Tuesday - Friday 8am - 7:00pm EST.
Your order confirmation is below. Thank you again for your business.

Your Order #100000063 (placed on March 9, 2010)

Billing Information:	Payment Method:
[redacted] Albuquerque , New Mexico, 87111 United States T: 5555555555	Check / Money order

Shipping Information:	Shipping Method:
#1 Customer 322 S. 5th St Quincey, Indiana, 62301 United States T: 5555555555	Fed Ex Smart Post - 4 - 14 Business Days

Item	Sku	Qty	Subtotal
FRYE LEATHER HANDBAG SZ OS	233497-e41[redacted]-S&B01	1	$0.99
		Subtotal	$0.99
		Shipping & Handling	$8.92
		Grand Total	**$9.91**

Thank you again,
MJR Sales
Find MJR Sales on Facebook! Follow MJR Sales on Twitter!!

Figure 08-04: Online Transaction Confirmation

Online Banking

Online banking is the method of making bank transactions or paying bills **over the Internet**. Online banking allows the user to make deposits, withdrawals, and pay bills with a single click of the mouse. Transactions are carried out electronically. **World Wide Web** (WWW) **technology** allows for information located on machines around the world to be accessed as a single multimedia linked document with simple **point-and-click interactions**. These payments are made by sending unencrypted credit card and transferring information using a telephone or fax. To secure the payments, banks have also introduced the **card-based payment schemes** across the network. These payments are secured using the cryptography techniques.

Advantages and Disadvantages of Online Banking

Although online banking has revolutionized how banking is done, it has its pitfalls. Some advantages and disadvantages of online banking include:

Advantages:

- Online banking allows the user to perform transactions, pay bills, and check balances 24 x 7.
- Online banking is fast, efficient, and effective.

Disadvantages:

- Online banking sites can take a while to start up and can be tricky for beginners.
- The customer may have a doubt if his/her transaction was successful or not.

Credit Cards Payments

Credit cards are **plastic cards** used for shopping, online transactions, or withdrawing money from the credit line provided by a financial institution. The consumer has to take all of the necessary steps to ensure that the credit card information is not compromised. A credit card enables people to buy goods and services while making monthly payments to the credit company. They have valuable consumer protection under the law. Credit cards are accepted by major **mercantile entities**. They are useful in case of emergencies. Purchases made by credit cards can be withheld until the problem is resolved.

A credit card system is similar to a retail transaction, and a credit system is issued to those who use the system. Credit cards are used to utilize money on credit from financial institutions, whereas a debit card requires that money be deposited beforehand. Credit cards are still the **preferred means** for online purchases because of:

- Ease of use
- The ability to pay the bills at a later date

Credit cards are issued by a credit card issuing bank or credit union after verifying users' credentials. The cardholder consents to pay by signing a receipt with a record of the card details that indicates the amount to be paid or by entering a **personal identification number** (PIN) or **Card Verification Value** (CVV or CVV2).

Types of Credit Card Frauds

Credit card fraud is a theft and fraud carried out using a credit card or any such payment mechanism as a **fake source for fund transaction**. In a typical credit card fraud, the attacker unlawfully obtains the credit card number of an intended victim and uses it to make purchases online or by telephone. After gaining the card details, the fraudster uses that person's credit card or debit card for transactions or to purchase property over the Internet. These numbers can be obtained from:

- A credit card generator website
- An unscrupulous retail merchant retaining credit card numbers processed through a retail outlet and using them unlawfully
- Offenders who utilize skimming machines to record multiple credit card numbers via retail outlets
- Sourcing discarded copies of credit card vouchers via waste receptacles
- Hacking into computers where credit card numbers are stored

Some types of credit card fraud include:

- **Credit card mail order fraud:**

  In credit card mail order fraud, the offender gathers information about the card holder and sends a request to the bank for a new or replacement card.

- **Skimming/counterfeit credit card:**

  Skimming is a process of electronically copying authentic data on a card's magnetic stripe to another card without the original cardholder’s knowledge. It makes a duplicate copy of the credit card.

- **Chargeback fraud:**

  In chargeback fraud, a genuine credit card holder uses the card to purchase goods or services, and when the bank statements come, they call the bank and claim that they have never authorized the documented transaction.

- **Lost and stolen card fraud:**

  In lost and stolen card fraud, a credit card is physically stolen or lost and then used by the offender to gain access to the card.

- **CNP fraud:**

  In card-not-present (CNP), the offender obtains credit card details and purchases goods over the Internet or by telephone, fax, or email.

- **Cash machine fraud:**

  In cash machine fraud, the offender tampers with an ATM machine so that the user’s card gets stuck when inserted. He or she then tricks the user into entering the PIN in his or her presence. It also involves shoulder-surfing in which the offender watches the user enter the PIN by looking over the user’s shoulder.

- **Shoulder-surfing:**

  The offender oversees the user entering his or her PIN at the machine.

- **Identity theft on cards:**

  In identity theft on cards, the offender uses the fraudulently obtained personal information of the credit card holder to open or access credit card accounts.

Guidelines for Ensuring Credit Card Safety

Before You Shop

1. Check if the site is of a known business entity (e.g., GAP).
2. Check for a third-party seal of trust (e.g., VeriSign or eTrust).

3. Check reviews of other shoppers (e.g., **www.epinions.com**).
4. Review the privacy statement.
5. Use only one credit card for all your online purchases.
    a. This ensures that the user does not expose all his/her credit cards' information when shopping.
6. Keep records of your online transactions.
7. Do not share your credit card information with anyone.

While You Shop

1. Disclose only the required personal information. Be discreet.
2. Ensure that you are using a secure computer and site.
3. Adopt a strong password.
4. Use one-click shopping cautiously.
5. Check for a confirmation email after an online purchase/transaction/payment.

Securing Online Transactions

During online transactions, an account holder transfers money electronically to another account holder. For this, he or she has to provide account details, which can be risky. So, transactions must be done securely while online. Online transactions can be secured by using alternatives to credit cards:

Stored Value Cards and Smart Cards

Stored-value cards are plastic cards with a **monitory value encoded in the magnetic strip**. They are an effective replacement for cash and can be used for low-value retail purchases. They are different from debit cards. Stored-value cards are **not associated with the name of the user** and thus do not reveal any confidential of the user's information. Moreover, if a stored value card is lost, the consumer incurs a loss only to the extent of value that is still unused. Contrarily, debit cards are associated with the user's name and a losing a debit card may reveal the user's information.

Examples of stored value cards include payroll cards, government benefit cards, gift cards, and telephone cards. Stored value cards are divided into two types: one is **single-purpose cards** and the other is **multi-purpose cards**. Gift cards and telephone cards are examples of single-purpose cards. Multi-purpose cards are used for debit transactions such as withdrawing cash from **ATMs**.

A smart card is a credit card-sized plastic device that contains a silicon computer chip and memory. It can store, process, and output data in a secure manner. The smart card commonly stores cryptographic keys, digital certificates, identification credentials, and other information. It provides strong, two-factor authentication using the smart card and the PIN. It contains a microprocessor that differentiates it from the credit card, which has a magnetic strip. The data on the magnetic strip can be read, deleted, or even changed. Therefore, the **microprocessor** offers an extra layer of security. Smart cards can be used with a smart-card reader attached to a personal computer to authenticate a user.

The International Organization for Standardizations (ISO) uses the term "**integrated circuit card**" (ICC) instead of smart cards.

The smart card has dimensions of 85.6 mm x 53.98 mm x 0.76 mm. It is similar to ATM cards and credit cards. One important factor behind the smart card use is the fact that multiple applications are involved in the use of a smart card. A smart card provides portable, secure storage for digital certificates. The smart card can also be used for many applications, such as:

- Logon/logoff authentication of an operating system
- Authentication to a website
- Sending/receiving source email
- Encryption of data files

Digital Cash and E-Wallets

Digital cash is a method of **purchasing cash credits** in small amounts. The cash credits can be stored in a computer and spent when making electronic purchases over the Internet. The consumer can buy the credits from a financial institution. Digital cash is associated with a **serial number**, which can be used for online transactions. Entering the serial number does not give out any personal information. A **digital cash certificate** can be reused. Withdrawal, payment, and deposit are the three different transactions that are performed during digital cash procedure. Features of digital cash include:

- Security
- Anonymous
- Portable
- Recognizable
- Transferable
- Untraceable
- Infinite duration
- Divisible
- User-friendly

E-Wallet is a **software program** used for online transactions. It stores a user's password, credit card numbers, email contact, or social security number. E-wallet can be **downloaded** and **installed on a computer**, PDA, or smart phones. Some E-wallet software allows the user to store photos and maps. Billing and shipping information is mainly stored in E-wallet. Once the software is installed, personal information can be filled out in the E-wallet, which is stored. When the user orders something, the order form can be automatically filled using E-wallet. This helps to prevent the theft of personal information. It provides strong encryption for the stored data. E-wallet users should enter a password to open stored files. It also provides **better security features** such as a limit on wrong password attempts. When a user crosses that limit, he or she cannot logon. The disadvantage of E-wallet is that it includes threats such as:

- Adware, spyware, and Trojans
- User behavior tracking
- Cascading security breaches

Online Payment Services

Online payment services protect the privacy of online users. By using **third-party payment services**, one can make online payments and avoid giving his or her credit card information to the merchant directly. When using an online payment service, the user can transfer their money to an account associated with the online payment service. All purchases and/or transactions can be carried out through this account, thus eliminating the need to reveal one's credit card information or other personal details to the merchants.

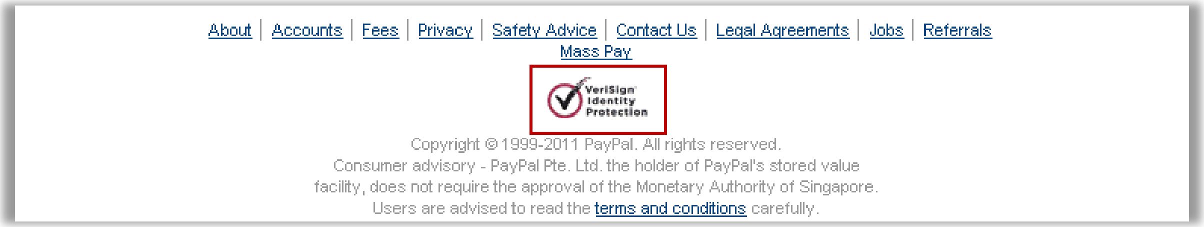
In a person-to-person (P2P) account, an account holder can transfer money electronically to the other account holder. Pay Pal is an example of a P2P payment service.

PayPal is one website for online financial transactions. It acts as a mediator for consumers and businesses. It provides a membership for the merchants who approach it. It is a trusted way of transferring money as it provides encryption for all credit card details through the **SSL connection**. It transfers money by sending the information via email. It provides two services; one is the pay-online service and the other is sell-online service.

Choosing a Secure Online Payment Service

A large part of business is conducted on the Internet. Bank and credit card accounts are the payment mediums. So, it is necessary to choose secure online payment services. Steps for choosing secure online payment services include:

- Ensure that the payment service is **legitimate/registered**
- Check the **reviews** of these services at websites such as **Epinions.com** or **BizRate.com**
- Look at the payment service's website for **seals of approval** from TRUSTe or Better Business Bureau Online (BBBOnline)
- Ensure that the website uses **encryption technology** to help protect the critical information
- The popular online payment services include PayPal, Amazon payments, and Google Checkout


About | Accounts | Fees | Privacy | Safety Advice | Contact Us | Legal Agreements | Jobs | Referrals
Mass Pay
VeriSign Identity Protection

Copyright © 1999-2011 PayPal. All rights reserved.
Consumer advisory - PayPal Pte. Ltd. the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore.
Users are advised to read the terms and conditions carefully.

Figure 08-05: Online Payment Service—Seal of Approval

Online Payment Services

PayPal

Source: https://www.paypal.com

PayPal is an e-commerce business allowing payments and money transfers over the Internet in a much safer and easier way. The service allows anyone to pay however they prefer, including credit cards, bank accounts, PayPal Smart Connect, or account balances, without sharing financial information.

Amazon

Source: http://www.amazon.com

Amazon is an online payment service that provides a safe means to process transactions online.

WorldPay

Source: http://www.worldpay.com

WorldPay is a global leader in payment processing. It securely processes online payments from face-to-face transactions to online and phone transactions.

2Checkout.com

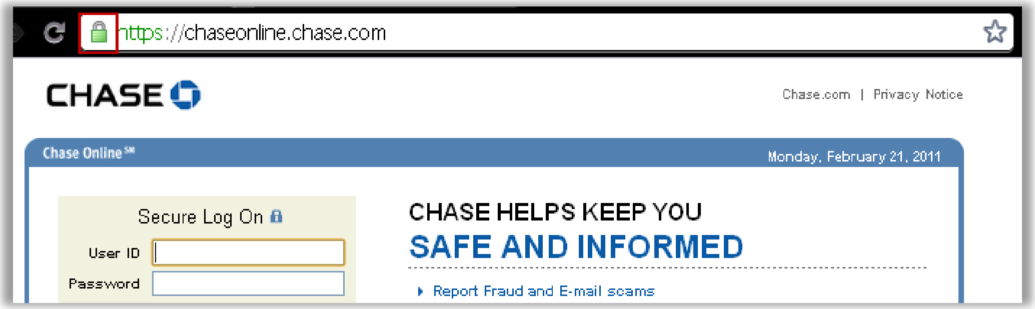
Source: http://www.2checkout.com

2Checkout's (2CO) payment and e-commerce services help you accept payments from a variety of credit and alternative payment types and help you manage fraud and credit card security so that your customers will keep coming back for many happy returns.

SSL and the Padlock Symbol

Secure Sockets Layer (SSL) is the standard **security technology** for creating an **encrypted link** between a web server and a browser. This link ensures that all information transmitted between the web server and the browser is secured. It uses a cryptographic system to encrypt the data with the help of both public and private keys. **Transport Layer Security** (TLS) is based on SSL. SSL uses the layer that is in between the Internet's Hypertext Transfer Protocol

(HTTP) and Transport Control Protocol (TCP). The padlock symbol is an indicator that the session is protected by SSL encryption.



https://chaseonline.chase.com

CHASE

Chase.com | Privacy Notice

Chase Online℠

Monday, February 21, 2011

Secure Log On

User ID

Password

CHASE HELPS KEEP YOU

SAFE AND INFORMED

Report Fraud and E-mail scams

Figure 08-06: Website for Creating a Safe and Informed Web Server Connection

What Does the SSL Show?

SSL protocol provides security to information transmitted through the Internet. It uses TCP to provide a **reliable** and **authenticated** connection among clients and servers in a network. SSL shows the:

- Domain name of the company
- Name and address of the company
- Details of the certification authority that issued the certificate
- Expiration date of the certificate

If the browser encounters an untrustworthy certificate authority, a site warning is displayed.

Identifying a Trustworthy Website

Guidelines for identifying a trustworthy websites:

- A secure site usually begins with the prefix **https.**
- The padlock symbol appears at either the bottom right in the browser or just beside the URL.
- The certificate that is used to **encrypt the connection** also contains information about the identity of the website owner or organization.
- Click the lock to view the identity of the website.

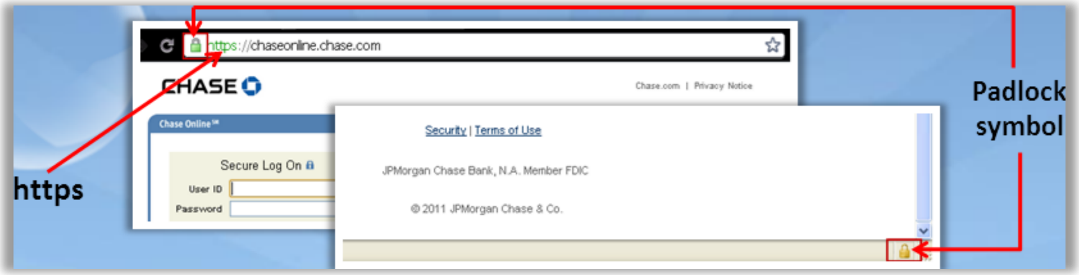
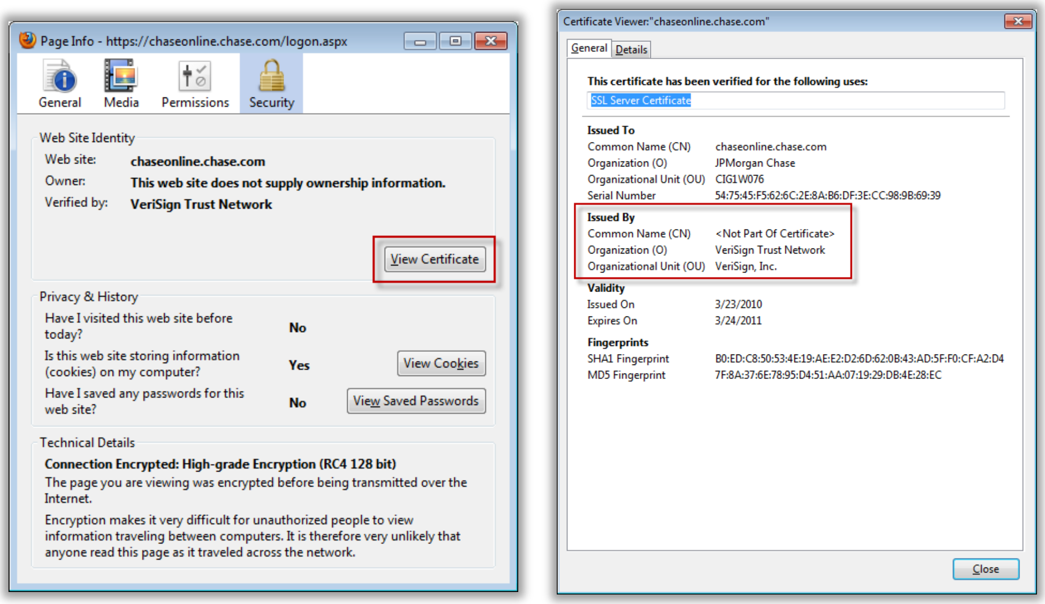

https://chaseonline.chase.com
CHASE
Chase.com | Privacy Notice
Chase Online℠
Secure Log On
User ID
Password
Security | Terms of Use
JPMorgan Chase Bank, N.A. Member FDIC
© 2011 JPMorgan Chase & Co.
https
Padlock symbol

Figure 08-07: Identifying a Trustworthy Website

- Clicking the padlock symbol reveals the website information.
- Click **View Certificate** to find the authenticity of the certificate.



Page Info - https://chaseonline.chase.com/logon.aspx

Web Site Identity

Web site: **chaseonline.chase.com**

Owner: **This web site does not supply ownership information.**

Verified by: **VeriSign Trust Network**

View Certificate

Privacy & History

Have I visited this web site before today? **No**

Is this web site storing information (cookies) on my computer? **Yes** View Cookies

Have I saved any passwords for this web site? **No** View Saved Passwords

Technical Details

Connection Encrypted: High-grade Encryption (RC4 128 bit)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

Certificate Viewer:"chaseonline.chase.com"

General | Details

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To	
Common Name (CN)	chaseonline.chase.com
Organization (O)	JPMorgan Chase
Organizational Unit (OU)	CIG1W076
Serial Number	54:75:45:F5:62:6C:2E:8A:B6:DF:3E:CC:98:9B:69:39
Issued By	
Common Name (CN)	<Not Part Of Certificate>
Organization (O)	VeriSign Trust Network
Organizational Unit (OU)	VeriSign, Inc.
Validity	
Issued On	3/23/2010
Expires On	3/24/2011
Fingerprints	
SHA1 Fingerprint	B0:ED:C8:50:53:4E:19:AE:E2:D2:6D:62:0B:43:AD:5F:F0:CF:A2:D4
MD5 Fingerprint	7F:8A:37:6E:78:95:D4:51:AA:07:19:29:DB:4E:28:EC

Close

Figure 08-08: Identifying a Trustworthy Website

Identifying an Untrustworthy Website

A website can be considered an untrustworthy website if:

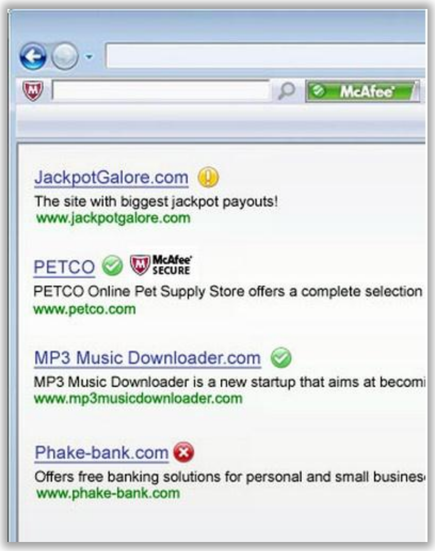
- The website is referred to users through an email message from an unknown source
- The website presents objectionable content, such as pornography or illegal materials
- The website offers schemes that seem too good to be true, indicating a possible scam
- The users are asked for a credit card as a verification of identity or for personal information even when not necessary

- The users are asked for credit card information without any proof that the transaction has been secured

McAfee's SiteAdvisor

Source: http://www.siteadvisor.com

McAfee's SiteAdvisor software is a free **browser plug-in** that alerts the user about the potentially risky sites that the user is about to visit. Once the software is installed, small site-**rating icons** are added to user search results. These site ratings are based on tests conducted by McAfee using an array of computers that look for various threats. The icons alert the user of the potential risky sites and help them find safer alternatives.



JackpotGalore.com
The site with biggest jackpot payouts!
www.jackpotgalore.com

PETCO ✓ McAfee SECURE
PETCO Online Pet Supply Store offers a complete selection
www.petco.com

MP3 Music Downloader.com ✓
MP3 Music Downloader is a new startup that aims at becomi
www.mp3musicdownloader.com

Phake-bank.com ✗
Offers free banking solutions for personal and small busines
www.phake-bank.com

Figure 08-09: McAfee's SiteAdvisor

Rating Icons

When the user installs the anti-virus, it enables/disables the rating ions. Some of the rating icons include:

- **McAfee SECURE:** Tested daily for attacker vulnerabilities
- **SAFE:** Very low or no risk issues
- **WARNING:** Serious risk issues
- **CAUTION:** Minor risk issues
- **UNKNOWN:** Not yet rated—use caution

Module Summary

The ease of shopping and comparing products and prices online has made online shopping an attractive option for consumers.

Online banking allows the user to make deposits, withdrawals, and pay bills with a single click of the mouse.

The consumer has to take all of the necessary steps to ensure that the credit card information is not compromised.

Using third-party payment services avoids giving your credit card information to the merchant directly.

The padlock symbol is an indicator that the session is protected by SSL encryption.

Online Transactions Security Checklist

The checklist to secure online transactions includes:

- □ Regularly update your operating system and other installed applications.
- □ Ensure that you have the latest web browser installed in the system.
- □ Ensure that you are connected to a secured network when using a wireless network.
- □ Regularly scan your system for viruses, worms, Trojans, spyware, key loggers, and other malware using updated anti-virus.
- □ Use strong passwords for all online transactions and change them regularly.
- □ Use Virtual Keyboard to enter sensitive information.
- □ Do not perform online transactions from public systems.
- □ Always completely log off after online transactions.

Online Transactions Security Checklist

The checklist to secure online transactions includes:

□ Never respond to unsolicited email offers or requests for information.

□ Use browser filters that warn about reported phishing sites and block access to those addresses.

□ Register for the bank's mobile alert service to get alerts whenever a significant transaction occurs.

□ Protect yourself from identity theft.

□ Always check the address bar for the correct URL.

□ Always check website certificate, SSL padlocks, and HTTPs.