Securing Online Transactions

Module 8

Simplifying Security.
OddJob, Zeus Mitmo Trojans Target Financial Data

Hide your bank account details, as two new pieces of banking malware are making the rounds: the OddJob Trojan, which keeps banking sessions open after users log out, as well as a variant of Zeus Mitmo that targets Symbian and BlackBerry smartphones.

On Tuesday, browser security firm Trusteer warned that the OddJob malware could keep banking Web site sessions open even after users thought they'd logged off. "By tapping the session ID token -- which banks use to identify a user's online banking session -- the fraudsters can electronically impersonate the legitimate user and complete a range of banking operations," according to a blog post from Amit Klein, CTO of security firm Trusteer.

Trusteer discovered OddJob several months ago, but withheld disclosing details until law enforcement agencies concluded related investigations. It said that the malware has targeted customers in the United States, Poland, and Denmark, and appeared to be the work of criminals based in eastern Europe.

http://www.informationweek.com
Module Objectives

- 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 SiteAdvisor
- Online Transactions Security Checklist
Online Shopping

Online shopping is the process of buying goods and services directly from the seller over the Internet.

The ease of shopping and facility to compare the products and prices online has made online shopping an attractive option for consumers.

The benefits of online shopping are:
- 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 travelling to the store using a credit/debit card
How Online Shopping Works?

1. Users visit the e-commerce site where they wish to buy goods/products from.

2. Users browse for the required product through the online catalogue.
How Online Shopping Works?

3. They add the product/service to the shopping cart.

The shopping cart shows:
- The products being purchased
- The number of units of the product
- The price of the product, taxes (inclusive/exclusive)
- Shipping costs, etc.

4. They fill in the online order form with:
- Shipping information
- Shipping address
- Consumer name
- Billing address and its details
- Credit card details
- Any other information the merchant requires
How Online Shopping Works?

1. The user’s credit card information is encrypted and sent to the merchant.
2. The user receives an on-screen confirmation or/and a confirmation e-mail.
Online Banking

- Online banking is the method of making **bank transactions** or paying bills **over the Internet**
- It allows the user to make deposits, withdrawals, and **pay bills with a single click of the mouse**

**Advantages**
- Online banking allows you to perform transactions, pay bills, and check balances **24x7**
- Online banking is fast, efficient, and effective

**Disadvantages**
- Online banking sites can take a while to start up and can be tricky for the beginner
- The customer may have a doubt that his/her transaction was successful
Module Flow

- Online Shopping
- Securing Online Transactions
- Identifying a Trustworthy Website
- How Online Shopping Works?
- Identifying an Untrustworthy Website
- Choosing a Secure Online Payment Service
- Online Banking
- SSL and the Padlock Symbol
- Online Transactions Security Checklist
Credit Card Payments

- Credit cards are still the preferred means for online purchases because of ease of use and the ability to pay the bills at a later date.
- The card user agrees to pay the card issuer the amount used for making the purchase.
- Credit cards are issued by a credit card issuing bank or credit union after verifying the user’s credentials.
- The cardholder indicates consent to pay by signing a receipt with a record of the card details and indicating 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 frauds refer to the acts of making purchases using someone else's credit card information.

<table>
<thead>
<tr>
<th>Credit card mail order fraud</th>
<th>Card-not-present (CNP) fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>The offender gathers information about a card holder and sends a request to the bank for a new or replacement card.</td>
<td>An offender obtains credit card details and then purchases goods and services over the Internet or by telephone, fax, or email.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Skimming/counterfeit credit card</th>
<th>Cash machine fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronically copying authentic data on a card's magnetic stripe to another card without the genuine card holder’s knowledge.</td>
<td>The offender tampers with the cash machine and then tricks the user into entering the pin in their presence.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chargeback fraud</th>
<th>Shoulder-surfing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genuine credit card holder uses the card to purchase goods or services, and when bank statements are issued, they call the bank and claim that they never authorized the transaction.</td>
<td>The offender oversees the user entering PIN at the machine.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lost and stolen card fraud</th>
<th>Identity theft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card is physically stolen or lost and then used by the offender.</td>
<td>The offender uses fraudulently obtained personal information of a credit card holder to access credit card accounts.</td>
</tr>
</tbody>
</table>
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, 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
6. Keep records of your online transactions
7. Do not share your credit card information with anyone

**While You Shop**

1. Disclose only required personal information. Be discreet.
2. Ensure that you are using a secure computer and using a secure 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

Online transactions can be secured by using the alternatives to credit cards.

1. Stored Value Cards
   - Stored-value cards are plastic cards with a monetary value encoded in the magnetic strip.
   - They are an effective replacement for cash and can be used for low-value retail purchases.
   - They are not associated with the name of the user, hence they do not reveal any information about the customer.
   - Even if lost, the consumer tends to lose only the value that is still unused.

2. Smart Cards
   - Smart cards are the same size as a credit card.
   - They have a microprocessor in them, which differentiates them from a credit card (which has a magnetic strip).
   - The data on the magnetic stripe can be read, deleted, or even changed.
   - Smart cards can be used with smart-card reader attached to a personal computer to authenticate a user.

Online transactions can be secured by using the alternatives to credit cards.
Securing Online Transactions

3 Digital Cash
- Digital cash is a method of purchasing cash credits in small amounts.
- Cash credits can be stored in your computer and spent when making electronic purchases on the Internet.
- The consumer can buy the credits from a financial institution.
- Digital cash is associated with a serial number that can be used for online transactions.
- Sending the serial number does not give out any personal information.

4 E-Wallets
- E-Wallet is a software program used for online transactions.
- Once the software is installed, personal information can be filled out in the E-wallet and stored.
- When the user orders something, the order form can be automatically completed using the wallet.
- This helps prevent the theft of personal information.
- By default, most of the electronic wallet software requests users to enter a password before completing the form.
Securing Online Transactions

5 Online Payment Services

- **Third-party** payment services can be used to make online payments to **avoid** giving away credit card information to the merchant directly.

- When using an online payment service, the user should **transfer money** to an account associated with the online payment service.

- All the **purchases** and **transactions** can be carried out through this account.
  - This way the customer does not have to reveal credit card information or other personal details to the merchants.
Choosing a Secure Online Payment Service

1. Make sure that the payment service is legitimate/registered

2. Check the reviews of these services at websites such as Epinions.com or BizRate.com

3. Look at the payment service's website for seals of approval from TRUSTe, VeriSign, or Better Business Bureau Online (BBBOnline)

4. Ensure that the website uses encryption technology to help protect your information
Online Payment Services

[Images of PayPal, Amazon, WorldPay, and 2Checkout websites]

- PayPal: https://www.paypal.com
- Amazon: http://www.amazon.com
- WorldPay: http://www.worldpay.com
- 2Checkout: http://www.2checkout.com
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.

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

Padlock Symbol
What Does the SSL Show?

- 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.
Module Flow

Online Shopping
Securing Online Transactions
Identifying a Trustworthy Website
How Online Shopping Works?
Identifying an Untrustworthy Website
Choosing a Secure Online Payment Service
Online Banking
SSL and the Padlock Symbol
Online Transactions Security Checklist
Identifying a **Trustworthy** Website

A secure site usually begins with the prefix **https**

The Padlock symbol appears either at the **bottom right** in the browser or **beside** the URL

The certificate used to encrypt the connection also contains information about the **identity of the website owner or organization**

The user can click the lock to view the **identity of the website**

**https**

Padlock symbol
Identifying a **Trustworthy Website**

Clicking the **Padlock** symbol reveals the **website information**

Click **View Certificate** to view the **authenticity of the certificate**

Certification authority
Identifying an **Untrustworthy** Website

- Untrustworthy websites are generally referred to the user through an email message from someone unknown.

- 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.

- When the user is asked for a credit card to verify his/her identity or for personal information when it's not necessary.

- When the user is asked for credit card information without any proof that the transaction has been secured.
McAfee’s SiteAdvisor software is a free browser plug-in that gives safety advice about websites before the user clicks a risky site.

Once the software is installed, small site-rating icons are added to the user’s 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 him/her find safer alternatives.

http://www.siteadvisor.com
Rating Icons

- **McAfee SECURE**: Tested daily for hacker 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 the 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 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 the SSL encryption.
Online Transactions Security Checklist

- 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 keep them changing at regular interval
- 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

- Never respond to unsolicited email offers or requests for information
- Use browser filters that warn about reported phishing sites and block access to the addresses
- Register for the bank's mobile alert service to get alerts whenever there is a significant transaction
- Protect yourself from identity theft
- Always check the address bar for the correct URL
- Always check for the website certificate, SSL padlocks, and HTTPS