Project Pro$per

presents

Protect Yourself Financially

Participant Guide

www.projectprosper.org

www.facebook.com/projectprosper

Based on Wells Fargo Hands on Banking ®

The Hands on Banking® program is a free public service provided by Wells Fargo. You may also access the program anytime at www.handsonbanking.org & www.elfuturoentusmanos.org
Table of Contents
MONEY SAFETY AND SECURITY TIPS ........................................................................................................ 1
  How can I keep my information safe at home? ....................................................................................... 1
  How Do I Keep my information safe on the internet? ............................................................................. 2
Financial Service Providers Can Help ..................................................................................................... 5
  What can I do to help? ............................................................................................................................ 5
ATM, Debit & Credit Card Security Tips .................................................................................................. 6
  Introduction to Fraud ............................................................................................................................... 8
  Two Common Fraud Examples ............................................................................................................... 8
  Phishing Activity ..................................................................................................................................... 9
Resources for Further Information and Assistance .................................................................................. 11
Glossary ....................................................................................................................................................... 12
Post Test ...................................................................................................................................................... 14

For more information about our small No-interest loan program for immigrants and refugees you can reach us at:
www.projectprosper.org
727-538-4179
Facebook.com/projectprosper
Join Our Facebook Group: Project Prosper: Money Talks
I. MONEY SAFETY AND SECURITY TIPS

A. The Basics

There are too many ways that dishonest people or a few businesses may try to take your hard-earned money. However, there’s a lot to learn about how to protect yourself financially – whether you’re on the phone, on the Web, at the store, or wherever your day may take you.

B. How can I keep my information safe at home?

A. Be wary of strangers you allow into your home.

- Keep SENSITIVE DATA, information you would not want anyone to see or take, out of sight. (i.e. driver’s license, bank statements)

B. Please list examples of sensitive data you would not want shared with others.

<table>
<thead>
<tr>
<th>1.</th>
<th>6.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>7.</td>
</tr>
<tr>
<td>3.</td>
<td>8.</td>
</tr>
<tr>
<td>4.</td>
<td>9.</td>
</tr>
<tr>
<td>5.</td>
<td>10.</td>
</tr>
</tbody>
</table>

C. Safely store_sensitive data in a lock box or secure place along with your new and bank statements.

D. SHRED old and unnecessary financial documents, statements, and unwanted credit offers. However, after you pay your taxes each year, don’t shred tax returns.
C. How do I keep my information safe on the internet-

A. Don’t send personal information such as account numbers, credit card numbers, or PINs via email.

B. Select one credit card with a low credit limit to use for all your online purchases.

C. Immediately after you make a Web transaction, completely close your browser.

D. Turn off your computer when you’re not using it – don’t leave it in “sleep” mode.

E. Never download files or click on HYPERLINKS in emails from people or companies you don’t know.
   - Hyperlinks = www.projectprosper.org

F. Install a FIREWALL, VIRUS PROTECTION, and SPYWARE on your computer and update them regularly.
   - Often times all three services will be provided in a package with the following services. Always call, email, or chat online to make sure.
     i. Norton Anti Virus Protection
     ii. MacAfee Virus Protection
     iii. Kaspersky Virus Protection

D. How To Know Which Websites Are Safe and Secure

1. To maximize Web transaction safety, use a recent version of your Web browser.
   a. Internet Explorer
   b. Google Chrome
   c. Mozilla Firefox
   d. Opera
2. Web addresses starting with “https” and web pages with a padlock symbol in the address bar are considered secure.
   a. For example, on your smart phone, please visit your bank’s website. Inside the address bar your bank address should read, https://www.yourbank.com. You should also see a closed lock in the address bar beside this address.
   b. Now visit one of your favorite shopping sites and you will see that the address bar reads http://www.yourfavoritestore.com

3. If it is a new business that you have never used before, you can always call them first and speak with a representative of the company or email them.

E. Use review websites to research businesses
   a. BETTER BUSINESS BUREAU is a useful website to use when you want to know if an online company has a good or bad reputation. Consumers, like you, use this website to grade services from A+ to F, and they also leave reviews. This helps you not do business with thieves, or bad business people. www.bbb.org
      i. Search for the business name and look for this symbol,
      ii. If you don’t see this symbol beside the business name then read the reviews carefully!
   b. YELP.COM
   c. Urbanspoon.com
   d. Epinions.com
   e. Ask.com
   f. Google.com

If you are unable to call, email, or find the business with the better business bureau, it is our suggestion that you be cautious about purchasing products or using the services of this business.

Tip!
Whenever you have the opportunity always read consumer reviews on business products and/or services. These reviews are mostly written by people like you and me who have nothing to gain or lose!
II. Financial Service Providers Can Help
When it comes to protecting yourself financially, remember that your financial services providers – such as your bank and other lenders – play a valuable role.

A. Bank Policies and Procedures
Financial institutions have policies to help protect you from fraud:

a) **ID Cards**
   a) When you make a transaction at the teller window, the teller will typically ask you to provide two forms of identification.

b) **Teller-customer service**
   a) The teller or customer service representative may ask you specific questions about yourself to confirm your identity.

c) **ATM/Debit card reader**
   a) You may be asked to swipe your ATM or debit card and enter your PIN while you’re standing at the teller window.

d) **Check deposits**
   a) When you make a deposit, you may have to wait a period of time before you can withdraw the money. Check with your bank to confirm their policies and procedures.

B. What can you do to help?

A. **Check your statements**
   1) Review your account statements as soon as you receive them. Notify your financial institution immediately if you notice errors or unauthorized activity.
   2) If your account statement is late in arriving, call your financial institution to find out why.
   3) Always keep your credit card purchase receipts (including online purchases) and check your credit card statements to make sure the purchase amounts are correct.
   4) Immediately dispute any charges you did not make by notifying your credit card provider.

B. **Consider online banking**
   1) Consider signing up for online banking. This will allow you to monitor your account activity at any time.
   2) Never tell anyone your online banking password and change it periodically.
   3) Don’t use your Social Security number as your online banking username or password.
III. ATM, DEBIT & CREDIT CARD SECURITY TIPS

A. At the ATM
1. Be alert and aware of your surroundings. Use ATMs located inside banks or supermarkets in well-lit public areas. Avoid using an ATM in out-of-the-way or deserted areas.
2. If someone has broken or altered the ATM, **DO NOT USE IT**. A criminal may have attached a “skimmer” to steal your financial information.
3. If a suspicious person offers help with an ATM, refuse and leave.
4. Put your money and ATM card away before you leave the ATM. **Always avoid showing your cash.**
5. Always verify that the amount you withdrew or deposited matches the amount printed on your receipt. **Always shred or destroy your ATM receipts before you throw them away.**

B. Deal with loss and theft
1. Report lost or stolen credit cards immediately to the issuing card company and report a lost debit card to your bank.
2. To respond quickly if your cards or ID are lost/stolen, make a chart that lists the credit card name, the financial institution, the account number, and the 24-hour customer service number. Be sure to store the list in a safe place. Never carry it with you.

<table>
<thead>
<tr>
<th>CREDIT CARD NAME</th>
<th>FINANCIAL INSTITUTION</th>
<th>THE ACCOUNT NUMBER</th>
<th>CUSTOMER SERVICE #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platinum Visa</td>
<td>Wells Fargo</td>
<td>4444-4444-4444-4444</td>
<td>1-800-555-6262</td>
</tr>
<tr>
<td>Master Card</td>
<td>HSBC Bank</td>
<td>5555-5555-5555-5555</td>
<td>1-800-777-7777</td>
</tr>
</tbody>
</table>
C. Care for your card

3. Sign your card on the signature panel as soon as you receive it.
4. If you want a merchant to check your ID for verification you can also write “See ID” on the back of your card.
5. Keep cards away from magnets (they can erase information on the cards' magnetic strip)
6. Newer credit cards in the U.S. have an imbedded microchip to make them safer and less vulnerable to fraud.

D. Treat cards like cash

1. Protect cards as if they were cash – never let them out of your possession or control.
2. Don’t leave your credit cards in your car’s glove compartment.
3. Don’t lend your cards to anyone, even family or friends. You are responsible for their use.
4. Always be sure to take your ATM card out of the ATM.

E. PIN safety

1. Memorize your PIN number.
2. **Never write down your PIN**, especially on the back of your card, or carry it with you in case your wallet is ever stolen.
3. **Never tell anyone your PIN**. You are the only person who needs to know it.
4. When selecting a PIN, **avoid picking a number that is easy for others to guess** – for example, your name, telephone number, date of birth, or any of these combinations.
5. **No one** from a financial institution, the police, or a merchant should ask for your PIN.

F. When shopping

1. When shopping, be sure that you get your card back after every purchase.
2. Keep copies of your sales receipts in a secure place.
3. Don’t volunteer any personal information when you use your credit card
4. Don’t put your driver’s license number on your checks.
5. Review your statements regularly to ensure there are no suspicious charges.
6. Contact your bank immediately if you see a charge you don’t recognize.
IV. INTRODUCTION TO FRAUD

A. The Basics

1. **FRAUD** is the many ways in which dishonest people may try to steal your money or identity.

2. When criminals obtain your credit, debit, ATM cards, or your personal financial information such as account numbers, passwords, or Social Security number, they can drain your bank accounts or make charges to your credit cards.

3. Criminals may also commit a crime called **IDENTITY THEFT**
   - When someone uses your sensitive data to take out loans, obtain credit cards and even driver’s licenses in your name.

4. Identity theft can seriously damage your credit and financial reputation, and it could take years to restore your good credit and name.

5. **Millions** of people have been identity theft victims in the United States. Don’t let it happen to you!

B. Two Common Fraud Examples

1. Fraudulent payments
   a) There are many variations on the fraudulent payment scam, but there’s a typical pattern
      i. Someone gives you money (via an electronic payment, check or money order) and then asks you to send some of the cash in return. When it becomes clear that the person’s story is fake and their payment fraudulent, you will have lost the money you sent them.
      ii. If you deposited the fraudulent check, money order or payment in your checking account, the deposit will be reversed and, as a result, you may discover that you have overdrawn your account.
   b) Examples of this scam include:
      i. **Work-at-home**: A company promises you easy money working at home. Then they ask you to help them by accepting a payment and then sending them money (minus your pay) via an electronic payment or money order.
      ii. **Overpayments**: You advertised an item for sale and the buyer “accidentally” sends you more than the price. The buyer then asks you to deposit their payment and send them the extra amount.
iii. **Sweethearts:** A special someone you’ve met online promises to come to the U.S. to be with you. They ask you to send them money directly or to deposit their check or money order and send them the cash to cover their travel expenses.

**Tip!**

*Immigrants and refugees can be at increased risk of being taken advantage of by family, friends, or strangers.*

2. **“Phishing” scams - Hi-Tech Fraud**
   a) When you receive an e-mail that asks you to contact the company immediately about your account by clicking on a link to their Web site:
      i. You’re likely to become a victim of fraud if you provide information to someone who requests it without double checking that the company is legitimate.
      ii. If you’re not sure whether you’re actually communicating with a company that you know and trust, don’t respond. This could be a "phishing" scam.
      iii. Contact the company yourself before you respond to an email that says “Immediate attention required” or “Please contact us immediately.”
      iv. When contacting the company, use contact information you know is genuine.

**Phishing Activity**

1. Sam receives a phone call from his local electric company. The customer service representative explains a special, time-limited offer on a new kind of light bulb that will cut Sam’s electric bill up to 80%. In order to guarantee his order, all he needs to provide is his customer account number, address, and a credit card number. She explains that due to the popularity of this offer, he must respond during this call or he’ll miss out. What should Sam do?

   _____ A. Sign up for the offer. It would be a serious mistake to pass up major savings on a monthly bill.

   _____ B. Use his credit card to buy the light bulbs, but don’t provide his customer account number.

   _____ C. Call the electric company directly using the phone number you know is correct.
2. Jena receives an email that states her immediate attention is required due to a serious problem with one of her credit card accounts. The message says if she doesn’t act quickly, her account may be closed and her credit record damaged. The email asks her to contact the company immediately about her account by clicking on a link to their Web site. What should Jena do?

_____ A. Click on the Web link and respond to the questions.

_____ B. Don’t click the link. Call the credit card company directly at the number printed on your card.

_____ C. Click on the link. Make sure the site looks legitimate. If so, provide the information requested.

If your personal or financial information is stolen...

C. Who do I contact?

1) Immediately contact your financial institution and credit card issuers and alert them to the situation.

2) You may have to contact your local police or sheriff’s department to make a formal complaint to the financial fraud department.

3) Contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file. This will help prevent thieves from opening a new account in your name.
   - Here is the contact information for each bureau’s fraud division:
     - Equifax 800-525-6285
     - Experian 888-397-3742
     - TransUnion 800-680-7289

4) Contact the FTC
   a) The Federal Trade Commission (FTC) works to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumer’s spot, stop, and avoid them.
   b) The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.
## Resources for Further Information and Assistance

<table>
<thead>
<tr>
<th>Resource</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Deposit Insurance Corporation (FDIC)</td>
<td>www fdic gov/consumers/consumer/guard/index.html</td>
</tr>
<tr>
<td>U.S. Postal Service Inspection-Identity Theft</td>
<td><a href="http://www.usps.com/postalinspectors/id_intro.htm">www.usps.com/postalinspectors/id_intro.htm</a></td>
</tr>
<tr>
<td>Anti-Phishing Working Group</td>
<td><a href="http://www.antiphishing.org/index.html">www.antiphishing.org/index.html</a></td>
</tr>
<tr>
<td>Police/Sheriff's Office Financial Fraud Department</td>
<td>Pinellas County Sheriff 727-582-6200</td>
</tr>
<tr>
<td></td>
<td>Hillsborough County Sheriff 813-247-8555</td>
</tr>
<tr>
<td></td>
<td>Pasco County Sheriff 727-847-8102</td>
</tr>
</tbody>
</table>
Glossary

ATM (Automatic Teller Machine)
a machine that dispenses cash or performs other banking services when an account holder inserts a bank card or credit card.

Federal Trade Commission
a federal agency, established in 1914, that administers antitrust and consumer protection legislation in pursuit of free and fair competition in the marketplace.

Fraud
Intentional use of deceit, a trick or some dishonest means to deprive another of his or her money, property or legal rights.

Firewall
a part of a computer system or network that is designed to block unauthorized access while permitting outward communication.

Identity theft
A criminal activity involving stealing personal information from others and forging their signatures in order to apply for credit in their names.

Log off
To stop a computer that is connected to a computer system or program.

Malware
software that is intended to damage or disable computers and computer systems.

Phishing
Is usually a two-part scam involving email and spoof websites. Fraudsters, also known as phishers, send email to a wide audience that appears to come from a reputable company requesting personal information and account numbers. This is known as a phish email.

PIN (Personal Identification Number)
an identifying number allocated to an individual by a bank or other organization and used for validating electronic transactions.

Secure browser
Websites or web programs that use encryption to protect customer data such as your name, addresses or account information.
Shred

a machine or other device for shredding something, especially personal documents that contain sensitive information.

Skimmer

A device that captures your debt card or credit card information so that it can then be used illegally.

Spyware

software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.
Protecting Yourself Financially  
Post Course Survey

Please answer the following questions. When finished remove this paper and hand it to our instructor. Thank you for attending our class!

1. A good way to find out if a company has a good or a bad reputation is to:
   
   □ Ask the company's salesman if they get many complaints?
   
   □ Only shop where you know the business?
   
   □ Check with the Better Business Bureau?
   
   □ I don’t know

2. When shopping online, you should not enter your private information unless:
   
   □ The webpage starts with https://and has a closed lock.
   
   □ A statement on the webpage says it is secure.
   
   □ The seller offers a great price for what you want to buy.
   
   □ I don't know

School Name__________________________________________