# SCAMS AND SCHEMES

WHAT IS IDENTITY THEFT,

AND HOW CAN YOU PROTECT YOURSELF FROM IT?

COMMON SENSE EDUCATION

# SCAM

- DO YOU KNOW SOMEONE WHO HAS BEEN SCAMMED? WHAT HAPPENED?
- WHAT IS THE PURPOSE OF A SCAM? WHAT TRICKS DO PEOPLE USE TO CARRY OUT A SCAM?
  - THE ULTIMATE PURPOSE OF A SCAM IS TO GET SOMEONE TO GIVE THE SCAMMER MONEY, OR INFORMATION THAT CAN HELP THE SCAMMER STEAL MONEY, SUCH AS A CREDIT CARD NUMBER, ATM CODE, OR PASSWORD
  - SCAMMERS TELL LIES AND OFTEN PRETEND TO BE SOMEONE THEY ARE NOT!
- CAN PEOPLE GET SCAMMED ON THE INTERNET? HOW?
  - SOMEONE CAN BE TRICKED INTO BUYING A BAD OR FAKE PRODUCT ONLINE (ME)
  - SOMEONE CAN BE LURED INTO SHARING INFORMATION THAT A SCAMMER CAN THEN USE TO STEAL FROM THEM.

# IDENTITY THEFT

- PEOPLE WHO SCAM OTHERS ONLINE DON'T ALWAYS HAVE TO GET MONEY DIRECTLY
- INSTEAD, THE USE A VARIETY OF STRATEGIES TO TRICK PEOPLE INTO GIVING OUT PRIVATE INFORMATION. THEY THEN USE THIS INFORMATION TO ACCESS THEIR BANK AND CREDIT CARD ACCOUNTS OR OTHER PERSONAL ACCOUNTS
- THEY CAN EVEN "RECREATE" SOMEONE'S IDENTITY AND PRODUCE FALSE DOCUMENTS, SUCH AS SOCIAL SECURITY CARDS, CREDIT CARDS, OR DRIVERS' LICENSES IN SOMEONE ELSE'S NAME
- IDENTITY THEFT – A TYPE OF CRIME IN WHICH A PERSON'S PRIVATE INFORMATION IS STOLEN AND USED FOR CRIMINAL ACTIVITY

# IDENTITY THEFT

- WHAT KINDS OF PERSONAL INFORMATION DO IDENTITY THIEVES LOOK FOR?
  - FULL NAME
  - DATE OF BIRTH
  - PLACE OF BIRTH
  - CURRENT AND PREVIOUS ADDRESS/PHONE NUMBER
  - DRIVER'S LICENSE OR PASSPORT NUMBER
  - ACCOUNT NUMBERS AND THE COMPANIES WHERE THE ACCOUNT IS (AMAZON, PAYPAL…)
  - PASSWORDS
  - SOCIAL SECURITY NUMBER

# VULNERABLE

- VULNERABLE – TO BE IN A POSITION THAT MAKES IT EASIER FOR YOU TO BE HARMED OR ATTACKED
- ANYONE IS VULNERABLE TO AN ONLINE SCAM, HARD TO BELIEVE BUT EVEN ADOLESCENTS AND TEENS
  - IDENTITY THIEVES LOOK FOR "CLEAN" SOCIAL SECURITY NUMBERS THAT HAVEN'T YET BEEN USED TO GET CREDIT. TEENS AND KIDS ARE TARGETED BECAUSE THEY OFTEN HAVE NO CREDIT HISTORY. IDENTITY THIEVES MIGHT SELL OR USE THESE NUMBERS, WHICH WOULD ALLOW SOMEONE ELSE TO GET A CREDIT CARD OR LOAN AND BUILD UP DEBT UNDER YOUR NAME.

# VICTIM

- BEING A VICTIM OF IDENTITY THEFT CAN RUIN YOUR FINANCIAL FUTURE AND YOUR ABILITY TO OBTAIN LOANS AND PURCHASE THINGS
  - FOR EXAMPLE, IT COULD AFFECT YOUR ABILITY TO GET A STUDENT LOAN FOR COLLEGE OR A LOAN TO BUY A CAR
- IN ADDITION, IF YOU USE YOUR PARENTS' ACCOUNTS AND CREDIT CARDS ONLINE, OR FILL OUT FORMS WITH YOUR PARENTS' INFORMATION YOU ARE SHARING INFORMATION THAT COULD POTENTIALLY PUT YOUR PARENTS' IDENTITIES AT RISK
- IT CAN TAKE MONTHS, EVEN YEARS, TO RECOVER A STOLEN IDENTITY
  - CLEANING UP SUCH A MESS TAKES A LOT OF TIME AND ENERGY AND IT CAN ALSO BE EXPENSIVE.

# HOW TO CATCH A PHISH

- HOW DO YOU THINK IDENTITY THIEVES MIGHT TRY TO GET INFORMATION?
- PHISHING – WHEN PEOPLE SEND PHONY EMAILS, POP-UP MESSAGES, SOCIAL MEDIA MESSAGES TEXTS, CALLS, OR LINKS TO FAKE WEBSITES IN ORDER TO HOOK A VICTIM INTO GIVING OUT PERSONAL AND FINANCIAL INFORMATION
- AVOID PHISHING SCAMS BY BEING SKEPTICAL ABOUT ANY ONLINE REQUEST FOR PERSONAL INFORMATION
    - DON'T TRUST ONLINE MESSAGES OR POSTS FROM FRIENDS THAT SEEM OUT OF CHARACTER FOR THEM, WHICH IS A WARNING SIGN THAT THEIR ACCOUNTS MAY HAVE BEEN HACKED.

# SPOTTING SCAMS

- **NEED TO VERIFY ACCOUNT INFORMATION**
  - PHONY EMAILS WILL TRY TO TRICK YOU INTO GIVING UP ACCOUNT INFORMATION OR PASSWORDS, OR CLICKING ON A PHISHING LINK WHERE YOU FILL OUT INFORMATION THAT IDENTITY THIEVES CAN COLLECT AND USE.
  - USUALLY WHAT THEY'RE ASKING FOR DOESN'T MAKE SENSE IF YOU THINK ABOUT IT, BECAUSE THEY SHOULD ALREADY HAVE THAT INFORMATION!

# SPOTTING SCAMS

- **SPELLING ERRORS**
  - SCAM EMAILS OFTEN INCLUDE SPELLING AND GRAMMATICAL ERRORS.
  - A REAL COMPANY WOULD NOT SEND OUT MESSAGES CONTAINING SUCH ERRORS

- **ALERT THAT ACCOUNT IS IN TROUBLE**
  - IDENTITY THIEVES TRY TO MAKE YOU WORRY THAT SOMETHING IS WRONG WITH YOUR ACCOUNT.
  - THIS WILL LIKELY MAKE YOU FEEL THAT YOU MUST IMMEDIATELY RESPOND TO THE EMAIL TO FIX IT.

# SPOTTING SCAMS

- **LINK IN EMAIL OR ATTACHMENT**
  - PHISHING EMAILS OFTEN HAVE A LINK WITHIN THE EMAIL OR AN ATTACHMENT THAT YOU ARE URGED TO CLICK ON.
  - THIS LINK CAN LEAD YOU TO A SITE OR FORM WHERE YOU (UNKNOWINGLY) GIVE YOU INFORMATION TO CRIMINALS.
  - YOU SHOULD NEVER RESPOND TO OR CLICK ON LINKS IN SUCH EMAILS.
  - INSTEAD, GO DIRECTLY TO THE MAIN WEBSITE OF THE COMPANY YOU HAVE THE ACCOUNT WITH, AND CHECK YOUR ACCOUNT FROM THERE.

# SPOTTING SCAMS

- **TOO GOOD TO BE TRUE**
  - SCAM EMAILS OFTEN OFFER THINGS THAT ARE TOO GOOD TO BE TRUE.
  - FOR EXAMPLE, YOU HAVE WON FREE MONEY OR PRIZES!

- **GENERIC GREETING**
  - YOU MIGHT SEE A GENERIC GREETING THAT DOES NOT PERSONALLY ADDRESS YOU.
  - REPUTABLE COMPANIES SEND EMAILS WHERE THEY ADDRESS THEIR CUSTOMERS BY NAME.

# PROTECT YOURSELF

- **AVOID PHISHING SCAMS**
  - AVOID OPENING THE MESSAGE OR EMAIL IN THE FIRST PLACE.
  - DON'T CLICK ON ANY LINKS OR DOWNLOAD ANY ATTACHMENTS (THEY MIGHT CONTAIN VIRUSES OR SPYWARE)
  - DON'T REPLY
  - MARK AS "JUNK MAIL" OR "SPAM" FOR YOUR EMAIL PROVIDER, OR REPORT IT TO YOUR SOCIAL NETWORK SITE
  - IF YOU ARE CONCERNED AB OUT AN ACCOUNT YOU HAVE WITH A COMPANY, CONTACT ITS CUSTOMER SERVICE BY PHONE. MAKE SURE YOU VERIFY THE COMPANY'S CONTACT INFORMATION ELSEWEHRE ONLINE FIRST.

# REAL SCAMS

- CONSUMER FRAUD REPORTING
  - HTTP://WWW.CONSUMERFRAUDREPORTING.ORG/PHISHING_EXAMPLES.PHP

- FACEBOOK SCAMS
  - HTTP://WWW.HUFFINGTONPOST.COM/2011/05/22/FACEBOOK-SCAMS-HACKS-ATTACKS_N_864906.HTML

# REPORTING SCAMS

- IF YOU ARE THE VICTIM OF IDENTITY THEFT YOU NEED TO WORK WITH THE FEDERAL TRADE COMMISSION

- FORWARD UNWANTED OR DECEPTIVE MESSAGES TO THE FEDERAL TRADE COMMISSION AT SPAM@UCE.GOV SURE TO INCLUDE THE COMPLETE **SPAM** EMAIL. YOUR EMAIL PROVIDER. AT THE TOP OF THE MESSAGE, STATE THAT YOU'RE COMPLAINING ABOUT BEING SPAMMED.

# SPOTTING SCAMS

- EACH EMAIL IS AN EXAMPLE OF A PHISHING SCAM
- REVIEW THE FEATURES OF A PHISHING EMAIL
- THEN UNDERLINE ANY EXAMPLES OF THOSE FEATURES IN EACH OF THE THREE MESSAGES
- LIST THE FEATURES IN THE BLANK SPACES PROVIDED, AND DRAW A LINE CONNECTING THE FEATURE TO THE PART OF THE EMAIL IT RELATES TO

# THINK LIKE A PHISH

- YOU CAN PROTECT YOURSELF FROM INTERNET SCAMS BY LEARNING HOW IDENTITY THIEVES THINK
- CREATE A PHISHING EMAIL, OR SOME OTHER FORM OF ONLINE OR MOBILE SCAM, USING WHAT YOU LEARNED ABOUT PHISHING SCAMS
- CHOOSE AT LEAST FOUR FEATURES OF A PHISHING EMAIL
- SHARE WITH A PARTNER, SHARE WITH OUR CLASS