# Scams

**New Tax Form Scam:**
This year some people have received some IRS forms from their bank in their mailbox requesting some very sensitive information. The problem is that neither your bank, or the IRS sent them, but an identity thief did. By filling out the forms and returning them to the fax number they provide, you put your identity at risk. The forms ask for information like your name and address, your social security number, your date of birth, bank account numbers, PIN numbers, etc. If you give this information out, an identity thief has all they need to assume your identity and clean out your accounts. The fraudulent forms on the right are examples of those made to look similar to actual IRS forms.

The scam has been reported in several states across the country. If you receive one of these forms, DO NOT fill it out and return it. You should immediately contact the IRS hotline at 1-800-829-0433 and your local US Post Office and file a report. If you have already filled out the form and faxed it in, in addition to the IRS and US Postal Service, you need to file a police report with your local department.

**New Identity Theft Scam:**
You could become a victim to a new Identity Theft Scam and not know it. Consumers making purchases via the Internet have long known of the potential for their credit card numbers to be stolen if they do not purchase from a reputable company on a secure website. Recently, would-be Identity Thieves have now begun targeting retail department store customers, as well, in an effort to steal your credit card number and other identifying information.

**The scam works like this:**
You make a purchase at a department store using your credit card. As the clerk rings up your purchase, the phone next to the register rings. The caller identifies himself as store security and claims that security has reason to believe you are a suspect in a credit card fraud. The caller describes you physically to the clerk as if the caller was viewing you on the store closed-circuit security cameras. The caller then says he needs the clerk to verify the information on the card, including the name, credit card number, and expiration date. The caller may also instruct the clerk to ask for your address and social security number. If you provide this information to the clerk, the caller now has everything they need to know about you to steal your identity. See, the caller is not store security, but a con-artist. The caller obtained the clerk's direct extension and is calling it from a cell phone as they watch nearby.
How you can protect yourself:

You should never provide your home address and social security number to anyone while making a credit card purchase. The merchant has no reason to ask for it and you are not required to provide it. If a clerk begins to give your credit card and personal information out to someone over the phone, demand to know whom they are talking to and why. If you are not satisfied with their response bring the matter to the attention of the manager on duty, then contact your credit card company immediately to report what has happened.

This is a relatively new scam, but it is a clever one. The more you know about it, the less likely it is that you will become a victim!

**Internet Scams**
Beware of fake websites that request your personal information - See example below

**Skimming Scam**
You have just finished eating dinner at your favorite restaurant. You hand the waiter your credit card. The waiter returns in a few minutes with your credit card and receipt for the meal. This is how a nice evening at a restaurant normally ends but what you do not know is you have just become a victim of Identity Theft.

This waiter used a technique called Skimming. This is a technique used by Identity Thieves to gain access to your Credit or Debit cards. The thief uses a small hand held electronic device known as a "skimmer". This skimmer gathers the information that is embedded in the magnetic strip of your card.

In the scenario described above a waiter takes possession of your card and on the way to the register they swipe your card in their hand held skimmer. This process only takes a second. The skimmer then has the information stored that was embedded in the magnetic strip of your card. This information may include your name, address, credit limit, and Personal Identification number.

With this information the thief can use it to make counterfeit credit cards or make unauthorized purchases over the phone or Internet. Unfortunately there is no way to tell when your card has been skimmed. The most important step you can take is to review your statements for unauthorized purchases. There are numerous ways that this skimming device can be used so always review your statements carefully.

**IRS E-mail Scam**
Recently, there has been an email making the rounds on the Internet claiming con-artists, purporting to be the IRS, are conducting an e-audit of your return and they need your full name, address, and social security number sent to them via reply email. The forwarded email message is a warning against this scam, but there is a problem, the scam does not exist-at least not yet.

It caused enough concern, that for a time, the State of Michigan posted a warning about the scam on its Department of Treasury website. The IRS says that it has no knowledge of such a scam and that it did not send out any warning as the forwarded email suggests. Further, the IRS does not conduct e-audits or request such information via email or notify individuals of audits in this manner.

As a way to protect your identity, never send your personal information and social security number via email to anyone. This information could easily be used to steal your identity and cause unnecessary havoc for you.

**ATM Fraud Scheme**
With many of us taking vacations during this time of year, ATM (automated teller machine) usage tends to increase. ATM's can be a fast and efficient way of getting money while traveling. However, if we do not take precautions, they can also be an easy way for someone to steal your cash.

The latest ATM scheme involves a thin, clear piece of plastic. This plastic is inserted into the ATM where we would normally insert our cards. When someone tries to use the ATM, the machine is unable to read the card. This causes the ATM to continuously ask the user to re-enter their PIN (personal identification number). Meanwhile, the fraudster who put the plastic in the machine is standing somewhere nearby watching while the PIN is input over and over. Eventually the unsuspecting victim gives up thinking that the machine is broken and has kept their card. The thief will then remove the plastic and be able to enter the PIN and get cash from the victim's account.

To protect yourself from this scheme run your finger over the card slot to feel for the plastic. If the plastic is there you should be able to feel two points, which are used by the thief to remove it. If you do find the plastic or any other device report it immediately to the bank and the local police department.

**809 Area Code Phone Scam**
Recently, there has been an email going around the Internet advising people to never call the area code 809. Although not everything in the email forward may be accurate, the scam is real. There are some things that you should be aware of in protecting yourself.

This is an old scam that has been around for several years and still exists. AT & T and the Federal Communications Commission (FCC) acknowledge its existence and have posted warnings to consumers on their websites. The scam lures people to call certain telephone numbers in the 809 area code by sending them emails, faxes, or beeper messages. The messages advise the victim to call the number to get more information about a family member who has been arrested or injured, to claim a prize, to offer employment opportunities, etc. What the message does not relay to the victim is the cost of the call. The 809 area code is located in the Dominican Republic, thus making it an international call. While most phone numbers in 809 are legitimate, the ones related to the scam are set up as a pay-per-call service, much like a 900 number in the United States. The victim can be charged an exorbitant amount for the call. The victim can be charged hundreds of dollars for the call and they will not be aware of the charges until their phone bill arrives. Unfortunately for the victim, there is little that can be done to recover the charges incurred once the call has been made. Because the area code 809 is in a foreign country, United States Law protecting consumers does not apply. Since the victim actually made the call, they will be liable for the charges incurred.

There are some methods that you can use to protect yourself. If you do not normally make international phone calls, you can have your long distance provider place a block on your phone line for out-going International Calls. Typically, there is no charge for this service. Also, you should never call into an area code that is unfamiliar to you without verifying it first. You can

contact your long distance provider or operator and inquire about the location of the area code before making the call.

If you are a victim of this scam or a similar phone scam, file a complaint with the FCC and your phone service provider. Complaints should be filed in writing and mailed certified. It is important to be as specific as possible. Include dates, times, names of those whom you have spoken to at the phone company, and a thorough description of the events. The phone company may agree to waive the charges but they are not required to. The FCC does not usually investigate individual complaints, but they do track trends and use information collected by consumer complaints to influence their policies and regulations. For more information, you can contact the FCC at http://www.fcc.gov or at 1-877-382-4357.

**New phishing attack uses real ID hooks**
By Matt Hines

Story last modified Sun May 15 21:00:00 PDT 2005

Security researchers are reporting a new brand of phishing attack that attempts to use stolen consumer data to rip off individual account holders at specific banks.

Workers at hosted security services company Cyota are sharing the details of this more sophisticated form of phishing threat, which forsakes the mass-targeting approach traditionally used in the fraud schemes in favor of taking aim at individual consumers. The security company would not disclose the names of the banks involved in the attacks, but said that its list includes some of the largest financial-services companies in the nation.

According to Cyota, the phishing e-mails arrive at bank customers' in-boxes featuring accurate account information, including the customer's name, e-mail address and full account number. The messages are crafted to appear as if they have been sent by the banks in order to verify other account information, such as an ATM personal-identification number or a credit card CVD code, a series of digits printed on the back of most cards as an extra form of identification.

Phishing is a form of online fraud that has exploded in frequency over the last several years. Typically using large-volume e-mail campaigns, phishers try to trick people into sharing personal information that the thieves then sell or use to commit identity theft. The new breed of attack, however, could have a higher success rate because the e-mails present unsuspecting recipients with accurate information in a document that looks like legitimate bank correspondence.

Cyota co-founder Amir Orad said he believes that the criminals responsible for the personalized phishing attacks have purchased stolen consumer data from other individuals and are trying to get information that's even more sensitive to sell to someone else at a premium.

"The attacks take advantage of poor technological defenses and continued consumer vulnerability, and evidence the work of an organized group with real research-and-development resources," Orad said. "So far, the success rates that we've seen are amazing. People are

expecting to see a crude attack that tries to steal their information; they're not expecting to see this much real information as part of the attack."
Repairs under way for server speed tests

Orad said that Cyota has already taken down several sites related to the personalized phishing schemes, but indicated that many more such sites have appeared since. The company is advising consumers to avoid sharing any financial information online without first verifying that a request for such data was sent for legitimate purposes.

In another recent development, the March phishing trends report released by the Anti-Phishing Working Group found that the attacks are increasingly relying on so-called keystroke loggers, a form of malicious program, to garner consumer information. Rather than trying to direct people to fake Web sites that ask for personal information, keystroke phishers capture login names and passwords for online bank accounts when customers access the accounts via computer. The keystroke logger programs then forward that information to the attackers.