What to do if you think you are a victim of calling card or third-party phone fraud?

First, remember you can hang up.
However, if you think you have already been victimized, call your long distance telephone company. If you are an AT&T customer, call 1 800 222-0300 (ext. 273) and a representative will assist you immediately.

AT&T cares about you. Please listen carefully and be aware of phone fraud.

What to do if you encounter other types of phone fraud:

A number of organizations and government agencies can provide you with additional information or assistance. They include:

Alliance Against Fraud in Telemarketing: Write 815 15th St., NW, Ste. 928N, Washington, DC 20005, or call 202 639-8140.

Better Business Bureau: Call the local BBB or Council of Better Business Bureaus at 703 276-0100.

Federal Trade Commission: Send complaints in writing to: Federal Trade Commission, Correspondence Branch, Washington, DC 20580, or call 202 326-2402.

National Futures Association: Write 200 W. Madison St., Ste. 1600, Chicago, IL 60606, or call toll-free 1 800 621-3570 (in Illinois, 1 800 572-9400).

North American Securities Administration Association: Call 202 737-0900.

US Postal Service: For complaints about bogus mail order investments and purchases solicited by telephone, call the telephone number which may be listed in your telephone book under US Government, Postal Service.

This information is brought to you by AT&T

Who are the prime targets?

Anyone can be the target of phone fraud. A con artist looking for a victim doesn't care about your age, the color of your skin or your religion. However, older people are, by far, the most frequent victims.

To begin with, seniors are more likely to be at home to receive the call. Furthermore, they may have considerable savings or pensions swindlers would like to get their hands on. And, they may be more responsive to the pitch of a smooth talking con artist.

As the pioneer and leader in telephone communications, AT&T has a special interest in making certain that your telephone offers you security and well-being–not harm. Phone fraud hurts us all. It is both upsetting and troublesome.

This brochure has been prepared to alert you to some of the most frequently perpetrated phone frauds and to help you recognize the unscrupulous caller. It describes a number of different telephone scams and, most importantly, it provides you with some very practical tips on how to protect yourself against phone fraud.

Presenting 4 easy ways to prevent fraudulent use of your Calling Card:

1. Whenever possible, enter your Calling Card number manually rather than reading it aloud to an Operator. If you must read it aloud, speak softly. If available, use magnetic-card-reading public phones.
2. Check that no one is watching or listening when you punch in or read out your number. Stand in front of the phone so others can't see which digits you are entering.
3. Don't offer your Calling Card as identification.
4. Be sure to take the same security measures you would use to protect a credit or charge card.

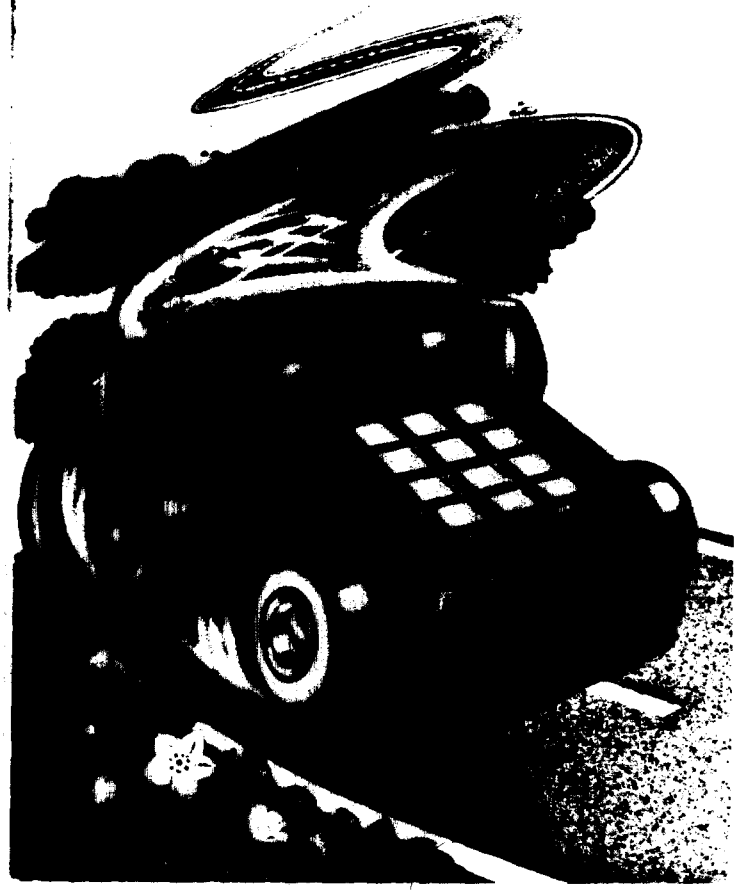
Representatives from AT&T or the local telephone company will never call you requesting verification of your PIN (Personal Identification Number), *so don't reveal it to anyone over the phone. If you need* more information, or if your card is ever lost or stolen, call toll-free, 24 hours a day: 1 800 CALL ATT. From outside the U.S., call collect: 1 816 654-6000.

AT&T

This advertisement is placed and paid for by AT&T. Pacific Bell has no affiliation with AT&T and cannot endorse, recommend or warrant any products or services described herein.

BE AWARE OF PHONE FRAUD

Wherever you are, you depend on the telephone to connect you with your family, friends and community. Unfortunately, con artists also depend on the telephone as their vehicle for conducting a variety of fraudulent schemes. You can avoid the dangers of phone fraud by watching for the caution signs mapped out in this AT&T brochure.



SCAM: Revealing your calling card number

Your calling card number is like money in the bank to scam artists who can use it to sell long distance calls to locations around the world. When you're making a call from a public phone, a thief may linger close by in order to hear you give your calling card number to the operator. He or she may also watch as you dial your calling card number.

Or, someone may call you at home posing as a telephone representative and ask for your calling card number to check on unauthorized charges, or to help trap a telephone scam artist.

DEFENSE:

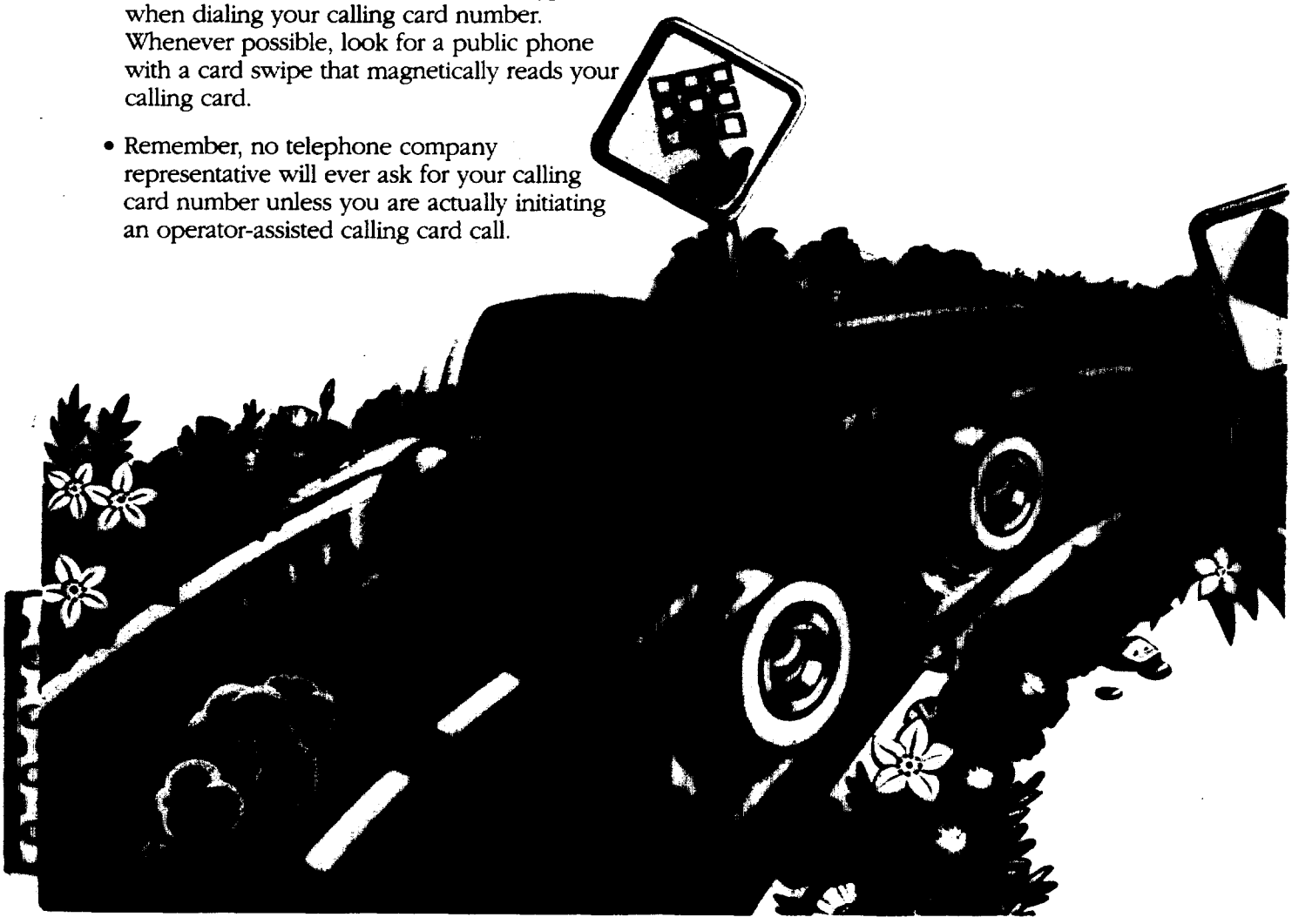
- When using a public telephone, look around before giving your calling card number to the operator. Speak directly into the mouthpiece in a quiet voice. Block the view of the keypad when dialing your calling card number. Whenever possible, look for a public phone with a card swipe that magnetically reads your calling card.
- Remember, no telephone company representative will ever ask for your calling card number unless you are actually initiating an operator-assisted calling card call.

SCAM: Disclosing your consumer credit card number

Some callers ask for your consumer credit card number in order to send you a prize or product you haven't ordered. Others ask to verify an insurance policy or charges on your credit card account.

DEFENSE:

Never give your consumer credit card number to anyone unless you are certain the request is legitimate – for example, if you are ordering products from a catalog or making hotel reservations. Don't ever reveal your credit card number as a means of identification.

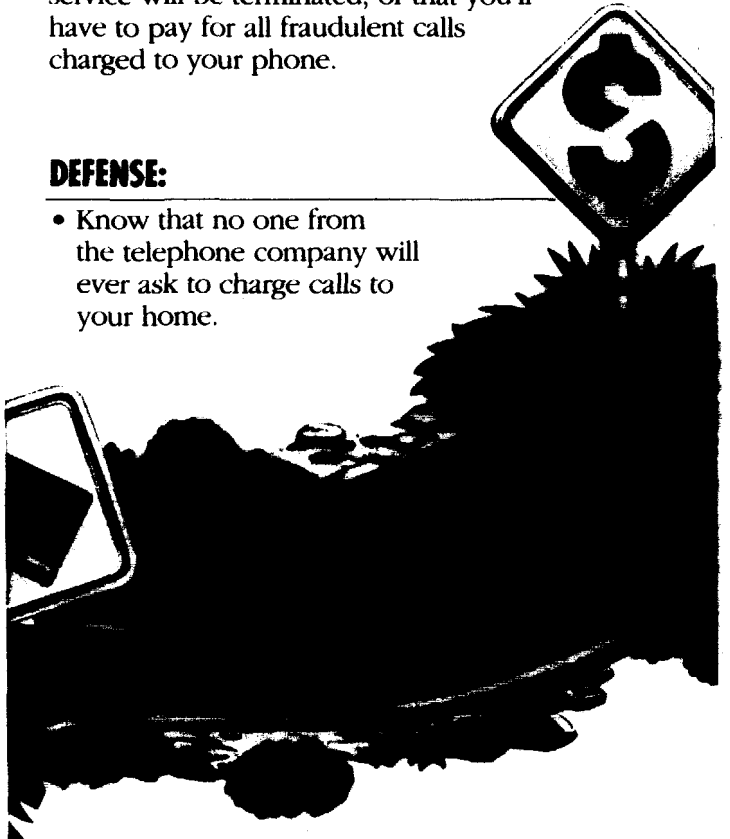


BE AWARE OF PHONE FRAUD

Wherever you are, you depend on the telephone to connect you with your family, friends and community. Unfortunately, con artists also depend on the telephone as their vehicle for conducting a variety of fraudulent schemes. You can avoid the dangers of phone fraud by watching for the caution signs mapped out in this AT&T brochure.

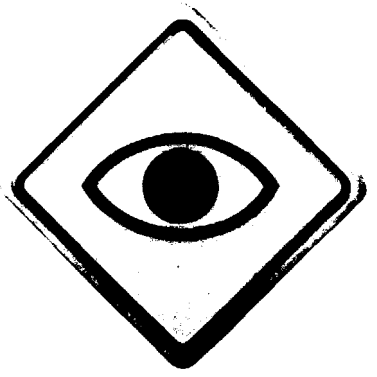
SCAM: Accepting toll charges for third party calls.

Your natural instinct to be helpful could entrap you in this costly scam. Here's how it works: Someone calls claiming to be a representative of the telephone company. The caller requests your help in an investigation by asking you to say "yes" when an operator calls to verify third-party charges (for toll calls made by someone else and charged to your number) for a specific period of time. You'll be assured you won't be charged for these calls. If you hesitate or seem reluctant to cooperate, he or she may say your telephone service will be terminated, or that you'll have to pay for all fraudulent calls charged to your phone.



DEFENSE:

- Know that no one from the telephone company will ever ask to charge calls to your home.
- Never accept third-party charges from anyone you don't know.
- You can be sure that AT&T – and other long distance companies – do not ask their customers to help trap telephone con artists.



10 TIPS FOR SPOTTING A SCAM!

Be suspicious if...

1. The company has a name that is intended to sound like a government agency or a well-known company.
2. You must act on the offer the same day.
3. The telemarketer acts like he or she has done business with you before.
4. The company is unwilling to send you written information on the offer or give you references.
5. The caller asks for your calling card number as identification for purchases.
6. Individuals linger close by while you are making a call from a public phone.
7. Someone claims you've won a prize – and you haven't entered a contest.
8. Someone asks for your calling card or credit card number to qualify you for a prize.
9. A telemarketer asks for your social security number so you can purchase products or

WHY IS AT&T CONCERNED ABOUT TELEPHONE FRAUD?

AT&T cares about YOU. As the pioneer and leader in telephone communications, AT&T has a special interest in making certain that your telephone offers you security and well-being – not harm.

HOW IS AT&T FIGHTING FRAUD?

To combat telephone fraud, AT&T has state-of-the-art systems in place to detect and deter many types of telephone fraud. But because the most effective safeguard against fraud is prevention, we're committed to educating consumers.

WHO ARE THE PRIME TARGETS?

Anyone can be a victim of phone fraud. A con artist looking for a victim doesn't care about your age, the color of your skin or your religion. However, older people, recent immigrants and non-English speaking people are the most frequent victims.

WHY SHOULD YOU BE CONCERNED ABOUT TELEPHONE FRAUD?

Phone fraud costs the telecommunications industry more than $2 billion a year – costs that are ultimately passed on to the consumer. So be aware – and protect yourself.

WHAT SHOULD YOU DO IF YOU THINK YOU ARE A VICTIM OF CALLING CARD OR THIRD-PARTY PHONE FRAUD?

First, remember you can hang up. However, if you think you've already been victimized, call your long distance telephone company.

If you're an AT&T customer, call 1-800-CALL ATT and a representative will assist you immediately.

WHAT SHOULD YOU DO IF YOU LOSE YOUR CALLING CARD?

Take care of your calling card as if it were a credit card. If you lose it, report the loss to your telephone company immediately. If you're an AT&T customer, call 1-800-CALL ATT and a representative will assist you immediately.

If you encounter other types of phone fraud:

A number of organizations and government agencies can provide you with additional information or assistance. They include:

National Fraud Information Center

800-876-7060

Better Business Bureau

Call your local BBB or
Council of Better Business Bureaus
703-276-0100

Federal Trade Commission

Washington, DC 20580
202-326-2222

National Futures Association

(For complaints regarding commodities only.)
200 W. Madison Street, Suite 1600
Chicago, IL 60606
800-621-3570 800-572-9400 (In Illinois)

North American Securities Administrators Association

To report incidents in your state:
202-737-0900

United States Postal Service

For complaints about bogus mail order investments and purchases solicited by telephone, call the number listed in your telephone book under US Government, Postal Service.

AT&T

Printed on Recycled Paper
©1993 AT&T
For additional copies call 1-800-851-0439

CUIDADO CON LOS FRAUDES TELEFONICOS

Dondequiera que esté, usted depende del teléfono para comunicarse con sus amigos o familiares. Desafortunadamente, los estafadores también dependen del teléfono para cometer una variedad de fraudes. Usted puede evitar los fraudes telefónicos siguiendo las señales de precaución que le brinda AT&T en este folleto.

FRAUDE: Dar a conocer su número de tarjeta telefónica

El número de las tarjetas telefónicas, que posibilitan hacer llamadas de larga distancia a crédito, como la tarjeta AT&T Calling Card, es muy valioso para los estafadores y estafadoras potenciales, ya que les permite vender a precio rebajado llamadas de larga distancia a diversos puntos del mundo. Para conseguir ese *número*, el estafador puede acercarse al teléfono cuando usted se lo dicta a la operadora, u observarlo cuando marca el número de la tarjeta.

Otras manera de conseguir ese número es llamándolo a su casa, haciéndose pasar por representante de la compañía de teléfonos. El estafador le pedirá el número con la excusa de que será usado para verificar facturas incorrectas o para atrapar a un estafador telefónico.

DEFENSA:

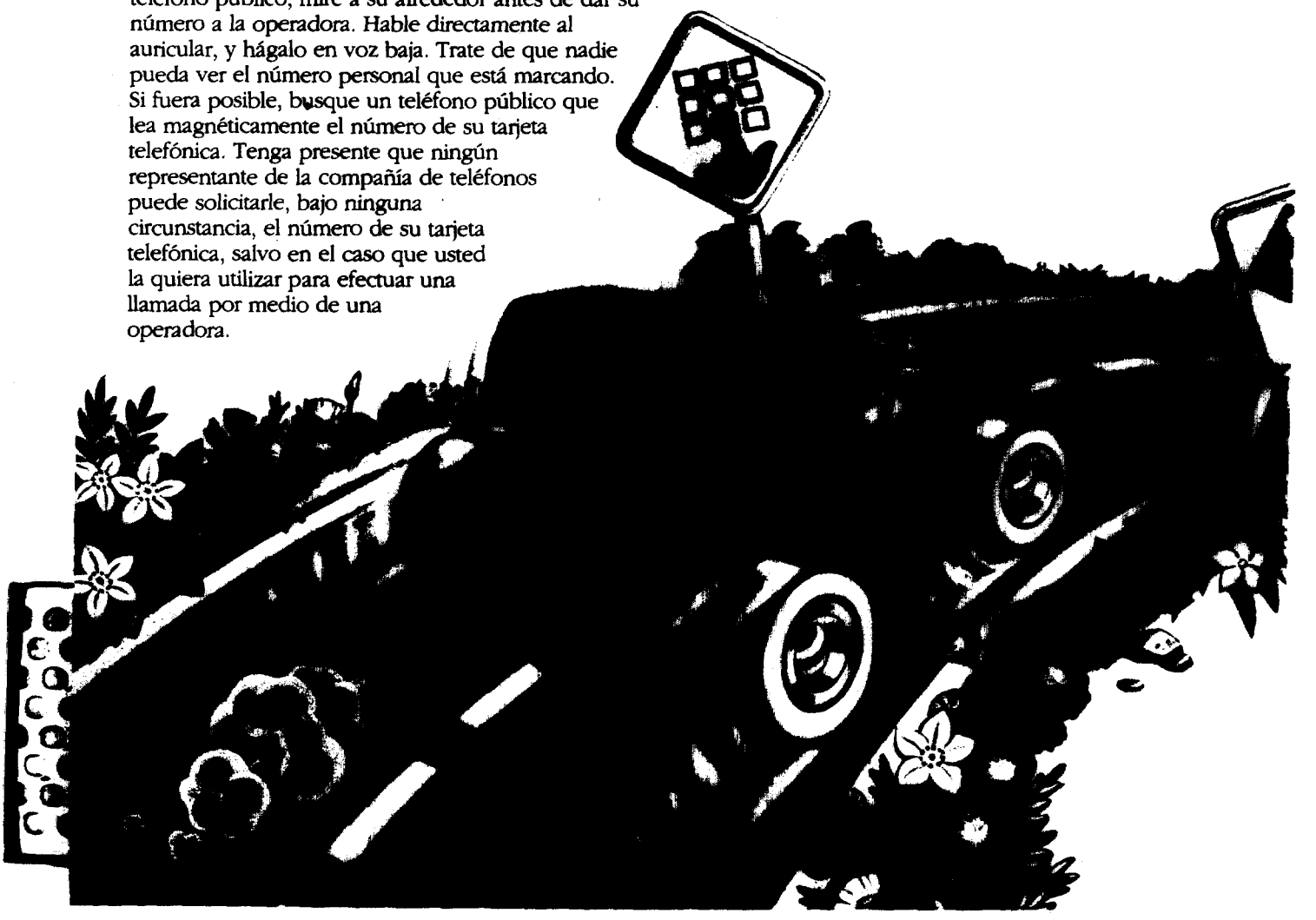
Cuando haga una llamada con tarjeta desde un teléfono público, mire a su alrededor antes de dar su número a la operadora. Hable directamente al auricular, y hágalo en voz baja. Trate de que nadie pueda ver el número personal que está marcando. Si fuera posible, busque un teléfono público que lea magnéticamente el número de su tarjeta telefónica. Tenga presente que ningún representante de la compañía de teléfonos puede solicitarle, bajo ninguna circunstancia, el número de su tarjeta telefónica, salvo en el caso que usted la quiera utilizar para efectuar una llamada por medio de una operadora.

FRAUDE: Dar a conocer su número de tarjeta de crédito

Alguien puede llamarlo para pedirle su número de tarjeta de crédito (como Mastercard, Visa u otras) con la excusa de que quiere enviarle un premio o un producto que usted no ha pedido. O le pueden decir que le llaman para comprobar su póliza de seguros, o los cargos de su tarjeta de crédito.

DEFENSA:

Nunca revele a nadie su número de tarjeta de crédito por teléfono, a menos que esté totalmente seguro de que es necesario, como, por ejemplo, si está ordenando un producto de un catálogo o haciendo una reserva de pasajes aéreos. Jamás dé a conocer su número de tarjeta de crédito como medio de identificación.



CUIDADO CON LOS FRAUDES TELEFONICOS

ndequiera que esté, usted depende del fono para comunicarse con sus amigos o ros. Desafortunadamente, los estafadores ón dependen del teléfono para cometer una iedad de fraudes. Usted puede evitar los udes telefónicos siguiendo las señales de ución que le brinda AT&T en este folleto.

FRAUDE: Aceptar el pago de llamadas de terceros

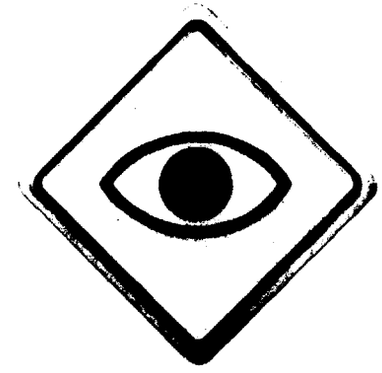
Su instinto natural de ayudar a los demás puede hacerle víctima de este costoso fraude telefónico. La estafa se desarrolla de la siguiente manera: Usted recibe una llamada de alguien que dice ser un representante de la compañía telefónica. El falso empleado o empleada le dice que necesita su ayuda para investigar y atrapar a un estafador telefónico.

Se le pedirá que diga "sí" cuando un verdadero empleado de la compañía telefónica le pida que apruebe las llamadas de terceros (o sea, las llamadas realizadas por otra persona y cargadas a su cuenta) durante determinado período de tiempo.

El estafador afirmará que esas llamadas no serán puestas en su cuenta. Si usted muestra señales de duda o rechazo, el estafador puede tratar de atemorizarle diciéndole que su teléfono puede ser desconectado, o que tendrá que pagar por varias llamadas realizadas por otros.

DEFENSA:

Esté seguro de que ningún empleado telefónico puede pedirle que ponga llamadas en su cuenta. Jamás acepte pagar por llamadas de personas que no conoce. Tenga presente que ni AT&T ni otras compañías telefónicas solicitan ayuda a sus clientes para atrapar a estafadores telefónicos.



DIEZ CONSEJOS PARA DESCUBRIR UN FRAUDE

Sospeche si...

1. El nombre de la compañía que se comunica con usted se asemeja al de una organización gubernamental o al de una empresa conocida.
2. Se le exige que acepte o rechace de inmediato lo que se le ofrece.
3. El vendedor telefónico actúa como si usted y él hubieran tenido tratos comerciales previos.
4. La compañía se muestra reacia a brindar información por escrito sobre lo que ofrece o darle cualquier otro tipo de referencias.
5. La persona que llama le pide el número de su tarjeta telefónica con la excusa de utilizarlo como identificación para sus compras.
6. Alguien se le acerca demasiado cuando usted realiza una llamada con su tarjeta telefónica desde un teléfono público.
7. Se le comunica que ha ganado un premio sin que usted haya participado en el concurso.
8. Alguien le pide su número de tarjeta telefónica o de crédito para tener derecho a un premio.
9. Un vendedor telefónico le pide su número de Seguro Social para que pueda comprar artículos o acceder a un premio.

¿POR QUE PREOCUPAN A AT&T LOS FRAUDES TELEFONICOS?

AT&T se preocupa por USTED. AT&T, una empresa pionera en los servicios telefónicos, tiene especial interés en que el teléfono le brinde a usted seguridad y bienestar, y que no sea un instrumento de daño.

¿COMO COMBATE AT&T EL FRAUDE?

Para combatir los fraudes telefónicos, AT&T cuenta con modernos sistemas que permiten detectar y desalentar diferentes tipos de fraudes. Pero como la mejor manera de evitar el fraude es mediante la prevención, AT&T ha adquirido el compromiso de mantener informados a sus usuarios.

¿QUIENES SON LAS VICTIMAS PRINCIPALES?

Cualquiera puede ser victima de un fraude telefónico. Cuando buscan a sus víctimas, a los estafadores no les importa la edad, el color de piel o la religión. Sin embargo, las víctimas más frecuentes suelen ser las personas de edad avanzadas, los nuevos inmigrantes y las personas que no hablan inglés.

¿POR QUE PREOCUPARSE POR EL FRAUDE TELEFONICO?

Este tipo de estafas le cuestan a la industria de las telecomunicaciones más de 2.000 millones de dólares por año. Y esos costos, en definitiva, los termina pagando el consumidor. De manera que sea precavido, y proteja sus intereses.

¿QUE DEBE HACER SI CREE QUE ES VICTIMA DE UN FRAUDE CON SU TARJETA TELEFONICA O DE COBRO DE LLAMADAS DE TERCEROS?

En primer lugar, recuerde que puede colgar el teléfono. Si cree que el fraude ya ha sido consumado, llame de inmediato a su compañía de llamadas de larga distancia. Si es cliente de AT&T, marque 1-800-235-0900, y recibirá de inmediato ayuda en español de un representante de AT&T.

¿QUE DEBE HACER SI PIERDE SU TARJETA TELEFONICA?

Cuide su tarjeta telefónica como si fuera su tarjeta de crédito. Si la pierde o extravía, haga de inmediato la denuncia a su compañía telefónica. Si es cliente de AT&T, llame al 1-800-235-0900, donde se le atenderá inmediatamente en español.

SI ES VICTIMA DE OTROS TIPOS DE FRAUDE:

Existen diversas organizaciónes y agencias gubernamentales que pueden proporcionarle información o asistencia adicional. Entre ellos:

National Fraud Information Center (Centro nacional de información sobre el fraude)

1-800-876-7060 (línea gratuita en inglés)

Better Business Bureau (Oficina que vela por la honestidad comercial)

Llame a su oficina local o a la sede central
1-703-276-0100 (en inglés)

Federal Trade Commission (Comisión Federal de Comercio)

Washington, DC 20580 1-202-326-2222 (en inglés)

United States Postal Service (Servicio Postal de los Estados Unidos)

Quienes deseen efectuar denuncias sobre solicitudes fraudulentas de inversiones por correo y productos o servicios ofrecidos por teléfono, deben llamar al número telefónico que aparece en su guía telefónica local, bajo "US Government, Postal Service".

CENTRO NACIONAL AT&T

Servicios en español durante las 24 horas
1-800-235-0900 (línea gratuita en español)

Impreso en papel reciclado

©1993 AT&T

APPENDIX B

OPTIONAL AT&T NetPROTECT(sm) OFFERINGS

AT&T NetPROTECT PLUS

For a one-time installation charge of $25 and a $10 monthly recurring charge, AT&T provides enhanced monitoring and notification services and will block outgoing calls upon detection of possible fraud, based on a prior written authorization from the customer. (Under AT&T's NetPROTECT Basic offering, AT&T cannot block calls until the customer has provided an authorization to AT&T after receiving notification of possible fraud.)

AT&T NetPROTECT Advanced

This option allows customers who subscribe to both inbound and outbound AT&T service, and who have certain types of CPE, to cap their liability for AT&T calls, provided that they implement prescribed security measures and give AT&T an approved list of originating telephone numbers. Other conditions and additional service charges apply to this option.

AT&T NetPROTECT Premium

This option is available to customers who use AT&T for all of their inbound service, meet all of the requirements of the NetPROTECT Advanced option, utilize longer passwords to protect their remote access feature (if any), and participate in a security review by AT&T. Customers who fulfill all of the above requirements are relieved of liability for fraudulent calls occurring prior to notification of possible fraud by AT&T.

SDN NetPROTECT

AT&T Software Defined Network ("SDN") service customers who subscribe to this option are provided usage information that allows them to track, in real time, the calls placed over their SDN service. Subscribers may notify AT&T of additional call blocking requirements, based upon their monitoring and detection of fraud in progress. Subscribers are not liable for fraud that occurs more than two hours after they notify AT&T of such additional requirements. They may also purchase separately SDN NetPROTECT Security Consulting Service for advice on how best to secure their network.

APPENDIX C

REQUIREMENTS FOR PPOs SEEKING TO AVOID LIABILITY FOR OPERATOR SERVICES CALLS

- The PPO must order OLS, BNS and international call blocking services from the LEC (or block or rate international direct-dialed calls in the phone) a reasonable period of time before the fraudulent calling occurred and retain appropriate written records of such service order;

- The blocking and screening capabilities must not have been discontinued due to the acts or omissions of the PPO, including termination or suspension of service for non-payment;

- The PPO has not taken any action to reduce the effectiveness of the blocking or screening capabilities, e.g., by adding an extension phone to the original line;

- The PPO has performed a prescribed set of test call within 5 days after the installation of new telephones to verify that screening and blocking capabilities have been properly implemented.[1] For all other phones, the PPO must have performed the test call procedures not less than four months prior to the occurrence of the fraud for which relief is being sought; provided that telephones which have previously experienced fraud due to failure of screening services shall be tested, at the request of the serving LEC, with every collection visit and not less often than monthly during the 90 days after such request. Coinless sets that do not require collection visits must be tested at least once every three weeks. The PPO must keep a written record of all such test results and promptly inform the LEC if any of the ordered services is not functioning properly.

- The PPO shall furnish written notice of claimed fraud to the LEC and applicable IXC(s) within 20 days of receipt of a bill for international calls and 45 days of receipt of a bill for domestic calls. Such claim shall include written documentation supporting the claim, including copies of applicable service orders and test call results.

---

1 The proposed test call procedures will be submitted separately by AT&T under confidential cover.

- The PPO must comply with reasonable requests from the LEC and/or IXC in connection with investigation of the alleged fraud