Sedona Police Department

Cons and Scams

Computer & phone phishing

Phishing is a scheme where criminals send a familiar-looking computer generated email message that contains a website link. Clicking the link sends the recipient to a fraudulent website that requests personal information such as a social security number, bank or credit card account numbers, or passwords. On the phone, a caller may try to entice you into believing the call is legitimate and will ask for personal information.

Never provide an unsolicited email or phone caller with personal information especially if the requestor appears to be a financial institution. Legitimate institutions will never ask for this information unless you initiated the call. If you get this type of email or telephone call, contact the business separately on your own. Do not ask them for a call back number because you will just end up calling the criminal back.

How thieves get your information

1. Coming into possession of your lost or stolen purse or wallet.
2. Stealing your mail or diverting it via a change of address request.
3. Getting into your trash and getting important documents.
4. Pretext calls where the thief poses as your bank, internet provider or other financial provider and asking you to "verify" or provide information.
5. Burglaries or vehicle break-ins where thieves steal records, wallets or purses.
6. Internet transactions on unsecured or fraudulent web sites.

Lottery scams

The letter/email indicates that you have won a lottery, usually from a foreign country and all you have to do is send a small fee to cover taxes and they will forward the money. Or you receive a cashiers check with a request to send them back a portion to cover taxes/handling fees. The checks are counterfeit.

The authors of this fraud are often overseas and the letters frequently contain grammatical errors or unusual phrases. Remember, if it seems too good to be true, it IS!

Some people represent themselves as successful individuals who are unable to remove their own money from their accounts because of the hostile government where they live. They request that you do something for them in exchange for money to be sent to you or ask you to set up a U.S. bank account or pick up packages for them. If you respond they'll try to convince you to wire money. Ignore these letters and emails.

Protect your information

- Protect your personal information. Never divulge personal information and account numbers over the phone unless you placed the call. If people ask you for personal information, ask why it's needed and how it will be protected.
- If your purse or wallet gets lost or stolen, minimize the damage. Don't carry more personal information than you need to carry. Don't carry your social security card in your wallet. Choose hard-to-guess passwords.
- Protect your incoming and outgoing mail. Have vacation mail held at the post office. Put outgoing mail into blue post office boxes, not your own mailbox.
- Keep thieves out of your trash. Use a cross-cut shredder to destroy any documents that contain personal information.
- Practice good home security. Store extra checks, credit cards and other financial documents in a document safe. Make arrangements to ensure your home looks cared-for and occupied during absences.
- Read your credit card and bank account statements. Check them monthly and look for discrepancies or unusual charges, missed payments and unauthorized withdrawals. Contact your provider if your statement doesn't arrive on time to make sure someone hasn't diverted your mail.

- Check your credit report once a year. The website annualcreditreport.com is the *only* free, federally-authorized site where you can apply for all three reports.
- Practice Internet safety. Look for secured sites (https) and keep passwords and PINs secured, and difficult to guess.

Identity theft prevention for businesses

Protect your clients/customers

Keep all documents containing personal information of your clients, customers and employees under lock and key.

When personal information is held within a computer, ensure that it can only be accessed and tracked by authorized personnel using passwords and is protected with an appropriate level of security/fire walls. When the information has been transferred to the computer, any handwritten information should be shredded.

Shred customer personal or account information and receipts before discarding them. Consider keeping shredders within reach of those employees who handle personal/account information on a regular basis.

Create policies to restrict the handling of customer information to a limited number of employees.

Customer personal information such as credit applications, sales receipts/carbon copies should not be temporarily kept within reach of the casual observer or other employees. Provide a secure receptacle for employees and citizens to throw out applications/receipts.

Protect your business from fraud

When accepting credit applications or checks, require the applicant to provide a finger print directly on the application or check. This aids law enforcement with identifying exactly who presented the documents.

Install video surveillance in areas where business is conducted with a loop time of at least one month. This will allow ample time for the fraud to be detected and the suspect transaction to be pulled for evidence. Video evidence combined with a finger print is very good evidence and reduces the possibility that employees would have to attend court.

Require a photographic ID be presented during check and credit card transactions, along with a finger print on the sales receipt and/or check. Inkless pads are readily available for each register.

If your business retails to other businesses utilizing a business account number and company credit card listed in your computer, understand that this information is often corrupted by ex-employees of the customer business. Always require that your sales representatives call a responsible party with the company to verify the transaction.

If your business accepts telephone or internet orders, always utilize the 3-digit verification number printed on the signature line of the card. This number should not be recorded on the internet order form or receipts generated from sales. This ensures that the card itself is in the possession of the customer and isn't being stolen from a discarded document.