

## **Scams, and how to avoid them**

If someone calls you and offers a deal that is too good to be true, it probably is! Nothing is free, including the cost of doing business. In fact, we want our vendors to make a reasonable profit...it ensures that we have a long relationship with reputable businesses.

The below information is offered to help our staff, faculty, and students identify and stop potential scammers. Many con artists depend on telephone sales as the vehicle to perpetrating fraud. The information in this section will enable you to be better prepared when encountering a potential scammer.

### **Your Best Defense**

Prior to releasing the names of our approved vendors to the university, the Purchasing Department takes every possible precaution in identifying companies that are stable, honest, and abide by our accepted business practices. Your best defense against becoming a victim of fraud is to immediately contact the Purchasing Department at (847) 578-8739, whenever you suspect that you have become the target of a scam.

### **What to Watch Out For**

Our preferred vendors should not attempt any of the following, so it's a good bet that someone attempting to do these is trying to scam you. Here are some things to watch out for:

- Offers requiring pre-payment of goods. (Any deals requiring a pre-payment should be coordinated with Purchasing prior to making any commitments.) This also applies to someone requiring pre-payment of shipping and handling costs.
- Company names that sound like a government agency or well-known company, but are not a company that you have dealt with in the past.
- Anyone claiming to be from the phone company, asking for your help troubleshooting a line or requesting information about an invoice.
- Someone calling for a survey, but cannot identify who the information is for, or what it will be used for. Usually, this is how scammers find information about other potential victims to further perpetuate their scams, or get your name so they can say YOU ordered the item.
- Offers requiring an immediate answer, or an answer that same day.
- Telemarketers who act like they have done business with you (or an associate) before, but you are not sure who they are.

- Companies who cannot send written information on an offer, or who try to pressure you into a sale before they will send the details in writing.
- Companies that call for copier count numbers, but cannot identify the make and model of the copier. If they are from the servicing company, they will have this information.
- Someone claims you've won a prize when you have not entered a contest.
- Someone who asks for a credit card number (or Social Security Number) as identification.
- Someone who requires a commitment for a certain quantity purchase over the phone.
- E-mail forms. Don't believe everything you read...e-mails can be easily forged, including the FROM information. Reputable companies do not engage in spam, do not contact their customers via e-mail for account information updates, nor do they use e-mail to verify security settings. However, they may contact you via e-mail and request that you contact the company. In that case, use the phone number or e-mail address from your most recent bill, not the information provided on the e-mail message.

#### How to Protect Yourself

Your first line of defense is to refer all callers to the Purchasing Department at (847) 578-8739. You can also follow up with a call to us directly, and let us know who is calling and why. That way, if we identify a scam, we can inform the other departments and better protect our university as a whole. Here are some other ways of protecting yourself:

- Ask all marketing, research, or charity callers to send you detailed, written information of any offers or surveys, so you can check it out for yourself. Request a paper catalog.
- Ask for written references, including names, addresses, and phone numbers.
- Only buy from vendors who you know personally.
- Ask for a name, an address, and a call-back number. This is not fool-proof, as scammers may work in teams, and may have someone standing by, ready to complete the con.
- Only buy from vendors pre-approved by the university. Call Purchasing (847) 578-8739 to verify if someone is an approved vendor, do not take their word for it.

- Read the small print. Fake invoices may be sent directly to you, requiring some piece of information to complete the transaction (address, name, etc.). Often scammers send a solicitation that looks like an invoice, hoping that you won't read the fine print at the bottom (or on the back). All invoices should be sent to Accounts Payable, not directly to you. Any company contacting you for payment on an invoice should be referred to Accounts Payable at (847) 578-8792.
- Know your rights. If you've received supplies or bills for services that you didn't order, don't pay for them, and contact the Purchasing Department immediately. This also applies to unauthorized substitutions in brand, quantity, size, or quality.
- Whenever someone offers you a sample, be clear that you are accepting it without any further commitment to buy any future products or services. If it's a free sample, do not pay for any shipping or handling charges. Companies will try to send you "free" items, and follow it up with an invoice, hoping you'll be too embarrassed to return the items. They may even try to pressure you into paying for them, telling you that they will ruin your reputation at that company if you don't pay.
- If you accidentally give out personal information, and realize you have made a mistake, you must immediately place fraud alerts to protect yourself from unauthorized transactions. You will want to call the three major credit companies place fraud alerts. You may also need to contact your bank and credit card company to report the fraud. They may require you to close your existing accounts and create new accounts.

Another venue is to contact the Federal Trade Commission (FTC) at [www.ftc.gov](http://www.ftc.gov) or at (877) FTC-HELP (877.382.4357).

## **Office Supply Scams**

Just because someone works for a well-known company does not make the salesperson reputable.

Here are some of the Office Supply Scams you may find:

### **The Current Vendor Approach (typically used for toner and printing supplies)**

The scenario is that you receive a call from someone claiming to be (or affiliated with) a current vendor for our university, and they have a special offer that they would like to tell you about. They proceed to describe a special offer on toner or printing supplies, but this offer is only good if you order it directly from them. Usually, these offers will only be valid if you act right away. If someone calls you claiming to be a current vendor, with an offer too good to pass up, it is probably a scam.

Another approach is that they claim to be checking on your supply of toner/printer ink, and want to know if they should send you some more. They may or may not give you a price, or they may claim it is “free” as part of the service. The giveaway is when they ask you for the model number. If they were really from your servicing company, they wouldn’t have to ask.

Once you actually receive the item, you find one of four things has happened:

1. The item costs several hundred dollars more than what seems reasonable.
2. The price of the item is not what you were told.
3. There is an excessive Shipping and Handling fee.
4. The quantity you are being billed for doesn’t match the quantity sent in the box.

Our vendors should not be calling you to solicit anything, at any time. This is not how our university does business, and our approved vendors will not do this.

### **The New Vendor Approach**

Occasionally, some businesses will try to approach the individual departments with specials and reduced pricing, to get their “foot in the door” at our university. Per university policy, any company who wishes to be considered for vendor status must do so through the Purchasing Department. Any vendor who calls you and tries to get you to buy a product or service should be directly referred to the Purchasing Department.

Legitimate businesses will honor our university policy and contact the Purchasing Department to introduce themselves. Although there is an accepted habit of “loss leading” (selling a product at or below cost to entice a new customer), there are other considerations that we need to evaluate. All of our potential vendors must successfully pass through several levels of screening, before we recommend them to our staff.

These factors include:

Price Are we really saving money by using this vendor? We not only consider prices, but payment terms, freight costs, delivery times (fill rates), return policies, and quality of merchandise.

Longevity Will they be in business tomorrow, in case we need to return defective merchandise or contest an erroneous charge? When a company goes bankrupt, we could be liable for orders placed to THEIR distributors, even if we already paid the company for the items. Our only recourse to get our money back from the bankrupt company is to sue them. We require a full financial disclosure of all vendors, before we allow them to sell their products to our university.

Experience Does this company have a record of success? If their prices are really low, they may have other problems that require them to constantly replace lost customers.

As you can see, the Purchasing Department takes every precaution in ensuring we deal only with legitimate businesses.

## **Computer Information Scams**

### **Phishing**

Phishing is the practice of using e-mail and spam to deceive customers into giving out names, credit card information, bank account numbers, ID/passwords, or other sensitive information.

The scammer hopes to cheat you out of some personal information, so that they can use your name and information to steal your identity, money, or internet access. The best way to protect yourself is to not give any personal information out through e-mail.

### **False-Front**

Scammers will use fake websites to force your internet browser to another site that looks like one you're searching for. These are very hard to detect, as they look exactly like the site that they are routing you away from. However, some tell-tale signs exist, if you are clever enough to check them out:

- Read the web address carefully. Look to verify that it's the site you were trying to reach. Be wary of names that look similar to the site you are trying to access, and make sure the extension is correct (.gov, .com, .org, etc.)
- If the web address doesn't begin with "https:", or there is no lock symbol at the bottom of your browser screen, it is not a registered, secured site, and most likely not genuine. However, some criminals are sophisticated enough to use encryption, so this is also not a sure-sign of a legitimate site.
- If other links on the site do not work properly, it may be a false-front. Be on the lookout for errors linking to other parts of a website. Legitimate businesses have tested their sites extensively before publishing them, and should not have excessive broken links.

This is not a complete listing of all possible scams, but should give you enough information to better protect yourself from being scammed.

If you would like to report a possible scam or get further information, please contact the Purchasing Department at (847) 578-8739.