Current Scam/Fraud Alerts

UW Supplier Alert

Alert to University of Washington Suppliers: Scam Directed Towards UW Suppliers

Suppliers, please be forewarned, ensure you are doing business with an authorized employee of the University of Washington.

The University of Washington has been experiencing numerous fraudulent emails to our suppliers posing as UW employees in an attempt to purchase items on behalf of the UW. The perpetrators of this scheme are requesting quotes not using typical UW processes to do so and are not using a valid University email address.

All University email addresses will end in either u.washington.edu or uw.edu. It is a rare occurrence for the UW to initiate a purchase by requesting a quote through email without providing:

- a valid UW Purchase Order Number
- UW delivery location
- UW department contact name and
- phone number

Please note that:

deliveries to personal residences are not allowed

- most of our purchases are going through our eProcurement system to UW registered suppliers on the Ariba network
- just as any business should do at a cash register, when accepting a payment method other than cash, proper identification should be obtained prior to completion of sale
- UW cannot be responsible for fraudulent orders or purchase orders
- if there is any doubt regarding the veracity of a purchase request, contact UW Procurement Services at 206-543-4500
- if a vendor accidently ships product as a result of being duped by this fraudulent scheme, they should report the incident to their local police department

For additional information regarding this fraud scheme, the FBI created a presention that has been modified for our specific use. This PowerPoint presention is very helpful for suppliers and UW Staff alike. Watch it here.

UW Weblogin Scam Alert

We are seeing a new bogus email appearing to come from UW Weblogin which announces irregular activity on your email account and requests that you log into a link that begins with weblogin.washington.edu.

This link is NOT related to the UW and appears to originate somewhere in Russia.

If you click on this bogus link, you get a replica of the UW weblogin page, designed to trick you into entering your UW NetID credentials.

If you have entered your credentials into this site, you should change your password at the valid UW site. You can go to the UW home page and search on "change password" or type this URL into your browser: https://uwnetid.washington.edu/manage/

If you have any questions, please contact UW IT at mailto:help@uw.edu or 221-5000.

Toner Phoner Phonies

Scammers are always trying to stay a step ahead of their potential victims, and recently we have seen an increase in phony toner sales calls, where the scam artist seems to have information on a recent order. These toner phoners are telemarketers who misrepresent themselves as Printer/Copier sales staff or as authorized representatives. They try to fulfill the order over the phone enticing the victim with better pricing for a short period of time prior to a companywide increase in toner cartridge cost.

If you are ever called by a salesperson that you aren't familiar with and asked to alter the standard purchasing process with that supplier, you need to be suspicious and deny the offer. And just as a reminder, never provide credit card, banking or personal information to anyone without being absolutely sure that it is a legitimate request and it's a secure transmission of the information.

DEPARTMENT OF REVENUE NEWS RELEASE

SuspectFraud.com helps consumers protect their pocketbooks

OLYMPIA – May 21, 2014 – "You pay; so should they. Report unregistered businesses." State agencies are using this theme to urge consumers to check with the state before hiring a business to do work for them.

Visiting suspectfraud.com before signing any contract can protect you, your property and potentially save you money. The site provides access to tools to verify a business is registered and licensed with the state. Consumers can check to see if a business is behind on taxes, has complaints filed against it or is subject to state enforcement actions. They can also report a business that they suspect is not following the rules.

The departments of Labor & Industries, Employment Security, and Revenue developed the website to give consumers a leg up when it comes to hiring a contractor, working with a business or paying for a

service. The agencies are promoting the suspectfraud.com campaign to raise consumer awareness during the months of May and June. The site is available year-round.

“During spring and summer many people hire contractors for outdoor home improvement projects like painting, adding a deck or putting on a new roof,” said Joel Sacks, director of the Department of Labor & Industries. “Hire Smart, and make sure any business that bids for your job is registered with the state and has a good track record.”

Everyone has a stake in tracking down businesses that fail to play by the rules. This underground economy creates an unfair advantage for law-abiding businesses; it’s also bad for consumers.

“Businesses that cheat the system may also cheat you,” said Dale Peinecke, commissioner of Employment Security. “When a company undercuts its competitors by not paying taxes or unemployment insurance, its low bid may look like a good deal. But that can be a sign of someone who will do shoddy work or, worse yet, take your money and run.”

The underground economy takes a bite out of the state’s budget, according to the Department of Revenue. Each year, unregistered businesses fail to report millions of dollars in taxes that would otherwise be used for schools, health care, child abuse prevention and other public services.

“In our efforts to track fraud, we discover businesses that collect retail sales tax but file false tax returns in order to keep the money for themselves,” said Carol K. Nelson, Revenue’s director. “When you or I pay taxes, we expect them to be used as intended. Checking suspectfraud.com is one resource to make sure a business is playing fair.”

Those who suspect a business is not registered, licensed or may be undercutting regulations are encouraged to visit suspectfraud.com and file a report.

Scam Awareness: Best Practices

Universities can be prime targets for scamming operations so beware of unsolicited communications from vendors you do not recognize as a UW supplier.

- Beware of suspicious sounding sales pitches, offers to send you a free product to “test” or calls from unknown vendors asking to verify your address.
- When contacted by companies claiming you owe money for goods or services you did not order, you should insist on written documentation of the purchase.
- Do not provide procurement card information or agree to pay invoices unless you are certain you ordered the item.
- If you receive supplies or bills for services you didn’t order, don’t pay, and don’t return the unordered merchandise. You may treat unordered merchandise as a gift.
- By law, it’s illegal for a seller to send you bills or dunning notices for unordered merchandise, or ask you to return it even if the seller offers to pay for shipping.

The FTC's Telemarketing Sales Rule requires telemarketers to tell you it's a sales call and who's doing the selling before they make their pitch. They must tell you the total cost of the products or services they're offering, any restrictions on getting or using them, and that a sale is final or non-refundable before you pay. It's illegal for telemarketers to misrepresent any information, including facts about the goods or services being offered.
If you believe you may be the victim of a SCAM, notify Procurement Customer Service by emailing pcshelp@uw.edu.

Looks Too Good To Be True?

Email is an inexpensive and popular method for distributing fraudulent messages to potential victims. According to the US Secret Service, hundreds of millions of dollars are lost annually and the losses continue to escalate. Most fraud is carried out by people obtaining access to account numbers and passwords. Never respond to any message that asks you to send cash or personal information.

A recent rash of email scams are making their rounds at the UW, of which two are particularly convincing because they appear to be work related. The first one sites a problem with a wire transfer, and if you're involved in transferring money via wire, it could lure you into following instructions that could compromise UW or your person information.

The second one is promoting toners at really, really cheap rates. If it sounds too good to be true**…..it is**. If you want, or need to advise a customer about some reasonably priced toner cartridges, Office Depot has remanufactured toner cartridges that will save you some real money. Go to eProcurement for more information and pricing.

One of the latest scams involves IRS Phishing. UW employees have been receiving unsolicited e-mails from the IRS. If you receive one, do not click on the link. Please forward any suspicious emails to phishing@irs.gov.

The FBI and the US Postal Inspection Service, along with other partners, have launched a web site to educate the public about Internet schemes and to provide a central place for consumers to file complaints. The site offers a novel interactive online fraud risk test that lets users measure online safety habits relating to identity theft, financial fraud, Internet auctions, counterfeiting, lottery scams, and computer privacy. It also provides prevention tips, details on current cyber scams, consumer alerts, victim stories, and an opportunity to share stories of cyber fraud. See Looks Too Good To Be True.