

# CITIZENS FRAUD UPDATE



These days, it can seem like an Olympic sport to try and keep yourself protected from scams. There are so many different tactics being used daily to try and trick people out of money or sensitive information with new tricks being tried all the time. You always need to keep your guard up and keep yourself educated on making smart choices when it comes to giving out information and purchasing items, especially online. In this newsletter, we will highlight some ways to protect yourself as well as highlight three significant fraudulent scenarios that our Citizens Connection team has had reported by clients this month. We recommend these 5 tips to keeping yourself safe from fraudulent activity and scams.



**RESEARCH:** Before you click, call, buy, or reply – do your research. Read over everything and hover over any links or websites. Google a company and see if the websites listed match. Look up the phone number given online or in a phone book. Do your own search on a phone number to reach a legit business instead of using the one listed. Look up reviews for any companies in question and see what other real customers have to say.

**THINK TWICE:** It's easy to get caught up when we are racing the clock, whether it be for a deal or a scare tactic that makes us think we are in a time sensitive, risky situation. However, you want to slow down and really think it through. Is this price too good to be true? Is this really the way a company would contact me? Do I really want to input my information on a place or platform that I am not familiar with?

**GUARD:** Keep your personal and financial information safe. Beware of where you enter your information. Always make sure that a site is secure before entering information. Never share your information with someone you don't know. Don't save your payment information online.

**REPORT:** If you are worried that you might have given financial or personal information out or been a victim of a scam, report it right away. Depending on the scenario you may need to call your bank, the credit bureau, Federal Trade Commission or the police.

**MONITOR:** Keep an eye on your bank account and make sure you can account for every transaction. Look into identity theft protection services that keep an eye on your credit and personal information.



*Citizens*  
BANK MINNESOTA

WoofHoo!  
Banking®



# TOP REPORTED FRAUD SCENARIO OF THE MONTH:

# SCAM SOCIAL MEDIA ADS

You're scrolling through and catching up on your social media when you see an ad that stops your scroll. A pair of shoes that you've had your eye on are on a MAJOR sale from a well-known retailer. Normally their \$150 price tag is a little outside of your budget but their sale price of \$29.99 has you feeling excited. You immediately click on the ad, find your size, and add to cart. This is your lucky day..... or is it? Spot the red flags below to see signs that it might be a scam social media ad!



**BEWARE OF "INFLUENCER" PAGES!**

Little Susie Shopper Group · Join

Guys, there's a HUGE sale going on over at Dick's Sporting Goods this weekend only! You can save up to 90%!! There are thousands of items available!


(ad) <https://go.sylikes.com/eMRbZXN1LV8d> limited time only

**HOVER OVER LINK TO SEE WHERE IT DIRECTS TO**



**LOW RESOLUTION OR LOW QUALITY LOGO**

**Updated Order ( 1 )**

 NithtKE DUNK LOW White/Black/US (W) /10 x 1	\$19.98 USD
Subtotal	\$19.98 USD
Shipping	\$8.99 USD
<b>Total</b>	<b>\$28.97 USD</b>

**BEWARE OF SPELLING & GRAMMAR ERRORS**



**THIS DOES NOT SEEM LIKE AN EMAIL AFFILIATED WITH THE COMPANY**

Any question? Feel free to contact us. We will do our best to provide you with a great shopping experience. If you have any questions or feedback, please contact [customers@goods-sales.com](mailto:customers@goods-sales.com)

# COMPUTER AT RISK POP-UPS

Another popular scam attempt we have been hearing a lot about is fake pop-ups appearing on their computer detecting that something is wrong. These fake pop-ups are usually after one of two things: to get you to click on a pop-up and install malware, or have you call a number to give out financial or personal information. Often these pop-ups will give you a sense of urgency that you need to act fast in order to prevent any danger.

How do I know if a pop-up is real or fake? In general, most of these pop-up type messages are fake and fraudulent. If you are worried about a possible virus, open up your anti-virus software and run your own scan to see if anything is detected. Other signs of fake pop-ups include:



**REQUEST OF PAYMENT** – If the pop-up requires you to make some form of payment, it is a scam.



**QUESTIONABLE DESIGN** – If the pop-up is very flashy with bright colors and exclamation points and block letters, it is most likely a scam attempt trying extra hard to scare you into taking quick action.



**CONTACT REQUIRED** – You do not need to call or respond to a virus threat or detection. A call will likely bring you to a fake call center where a scam artist will try to collect personal information or money to you.



## PROTECT YOUR COMPUTER AND YOURSELF

- Keep your computer up to date and make sure you are using the most current operating system.
- Install a high-quality ad blocker that prevents ads and pop-ups.
- Never click on a pop-up ad.

## WHAT DO I DO IF A POP-UP STOPS ME FROM CLOSING THE PAGE?

If you accidentally click on a pop-up you may be directed to a new page that overwhelms you with pop-ups and alerts. They have the ability to lock your browser which can stop you from closing the tab. Here are some ways to force an exit:

**Windows:** use Alt+F4 or Control+Alt+Delete – Select Task Manager and choose the program in which to End Task

**Mac:** Alt+Command+Escape or select Force Quit on the menu in top left corner.

# FAKE SHIPPING ALERTS VIA TEXT AND EMAIL

When ordering online, it can be common to receive email or text alerts about the status of your order and delivery. Fraudsters are trying to capitalize on this trend by sending out fake shipment alerts with a call to action in order to steal people's personal information. They want you to click on the link which leads to their look-alike website where they either steal personal information that's entered or get you to click on a link that could install harmful malware to your device. So how do you tell the difference between legit alerts and the scam alerts?

- If you receive a message about a package that you are not expecting, keep your guard up and do not click on any links from the message.
- If you are expecting packages and feel it may be a legitimate message, go straight to the source to check for alerts versus the message. Without clicking the bad link, navigate to the site you ordered from and check your order number that way.
- If you do click on a link that you are sure is legit, look closely at the details before entering in any information. Pull up the website and see if it matches 100% to what your alert says. Check for slight differences and spelling. Does it include a description of what you ordered and is it accurate?
- If you click a link and it's directing you to enter in personal information or pay money, do not take the next step.
- When in doubt, don't open or click. Get in contact with customer service from the company you are expecting the delivery from.

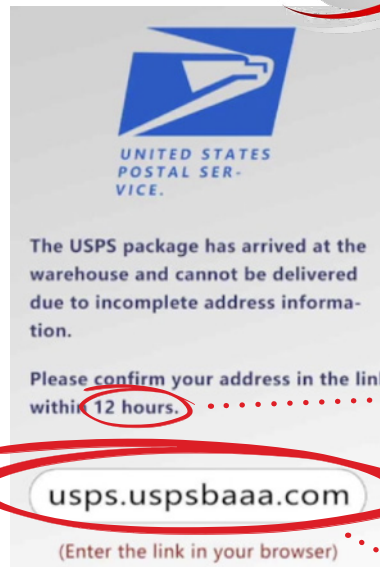


Hello Olivia, your FEDEX package with tracking code HB-6412-GH83 is waiting for you to set ~~delivery preferences:~~

[e3fmr.info/onAyXsfomA](http://e3fmr.info/onAyXsfomA)



**NOT A LINK TO THE REAL FEDEX SITE**



**CREATES SENSE OF URGENCY**



**NOT A LINK TO THE REAL USPS WEBSITE**