Office supplies are a critical and regular need for most offices. Scams related to phoned-in orders for such supplies are widespread and relatively common, yet many organizations still don’t know that these scams exist, much less how to identify and avoid them. There are several office supply scams out there, but we will address only the two most common scams identified by the Federal Trade Commissions (FTC). They are as follows:

**THE “HOOK”**

1. **Invoice Scams**

Scammers will do whatever they can to get the name of an employee who may have reason to order office supplies for a company, as well as that person’s postal or email address. Generally the fraudster will call the office and ask to speak to whoever orders office supplies because they need to complete an order previously called in. Once they have received the name and email address of the person who places orders, they can use that name to put on the invoice that they will be sending to the company in the future as “the authorized purchaser”.

But before they send the invoice, they will send the office unordered merchandise so that when they do send the invoice for the article sent at an outrageous price, the office will be more likely to pay it since they have already received the item. Confusion, bureaucracy, and lack of double checking on who may have ordered the unwanted goods are how the invoice generally gets paid. Often times when problems occur in an office setting that are too confusing, the invoice will just be paid to make it go away. And the scam artists are aware of that tendency. So be careful when you get a call at your office from someone saying they need the name of a person who orders office supplies to complete an order.

2. **The Pretender Scam**

In this scam, the scammer flat out pretends to a representative of your regular office supplier, or possibly identifies himself as a fill-in temporary replacement. By doing this, the victim becomes convinced that the office supplier’s services and products are being offered as usual, so it would seem normal to place an order to keep the goods in stock. It is inferred that the buyer would agree to the seller’s terms. The scam artist is hoping that topics such as pricing and brands will not come up, and if they do, the scam artist will beat around the bush and say things like “the prices will be the same as last time” or “let me look into that and get back to you”.

Another way scammers can pull off a fraud is to claim they want to send a promotional item free of charge. Once they get the name and address of the person at the office who normally orders business supplies, they send an invoice for goods that were never ordered or delivered. If the person at the office who pays invoices doesn’t double check to see who ordered the goods, and if they were received, it is likely they will pay the invoice.
THE LESSON

So how can you protect yourself from these scammers? It is very important to know your rights. The FTC states that *items received without being ordered can be considered a gift*. Therefore, you do not have to pay for them, and you don’t have to send them back! Also, you should train and educate all of your employees on how to handle suspicious phone calls, and what to look for.

Another way you can prevent these scams from happening is to assign a single designated buyer for all such purchases, make sure to record the purchase order (PO) number, and who needed the product at the office. This way the business can know what has been ordered, at what price, who ordered the goods, and if they were in fact received. This will help in any future audit of the books.

Always report any suspicious activities to the authorities. If businesses don’t report these scams they will continue to thrive. If possible, document and report any suspicious or fraudulent phone calls, invoices, or deliveries to both the authorities (your Attorney General and the FTC) and to your regular office supply vendor. Working together, businesses and legitimate suppliers can stop these con artists and report them to the FTC.

The information obtained to write this article can be sited at https://www.ftc.gov/.