INVESTAR Brilliant Banking Member FDIC

QUARTERLY NEWSLETTER

Shopping Online Securely

The information provided in this message is simply intended to help increase security awareness.

While many online stores are legitimate, there are some fake websites set up by cyber criminals. Criminals create these fake websites by replicating the look of real sites or using the names of well-known stores or brands. They then use these fraudulent websites to prey on people who are looking for the best deal possible. When you search online for the absolute lowest prices, you may find yourself directed to one of these fake websites. When selecting a website to make a purchase, be wary of websites advertising prices dramatically cheaper than anywhere else or offering products that are sold out nationwide. The reason their products are so cheap or available is because what you will receive is not legitimate, may be counterfeit or stolen, or may never even be delivered. Protect yourself by doing the following:

- When possible, purchase from websites that you already know, trust and have done business with previously.
- Verify the website has a legitimate mailing address and a phone number for sales or support-related questions. If the site looks suspicious, call and speak to a human. If you can't get a hold of someone to talk to then that is the first big sign you are dealing with a fake website.
- Look for obvious warning signs, like deals that are obviously too good to be true or poor grammar and spelling.
- Be very suspicious if a website appears to be an exact replica of a well-known website you have used in the past, but its domain name or the name of the store is slightly different. For example, you may be used to shopping online at Amazon, whose website is https://www.amazon.com. But be very suspicious if you find yourself at websites pretending to be Amazon, such as http://store-amazoncom.com.
- Type the store's name or URL into a search engine and see what other people have said about the website in the past. Look for terms like "fraud," "scam," "never again" or "fake." A lack of reviews can also be a sign indicating that the website is very new and might not be trustworthy.
- Before purchasing any items, make sure your connection to the website is encrypted. Most browsers show a connection is encrypted by having a lock and/or the letters HTTPS right before the website's name.

Remember, just because the site looks professional does not mean it's legitimate. If you aren't comfortable with the website, don't use it. Instead, find a well-known website you can trust or have safely used in the past. You may not find that absolutely amazing deal, but you are much more likely to end up with a legitimate product and avoid having your personal and financial data stolen.

For additional security information, please visit our website https://www.investarbank.com/learn. At the bottom of the page we have several topics you can read more about.
If you have any questions, please contact the Online Banking team toll-free at 855.306.8574 or email ebanking@investarbank.com. Thank you!