CYBER MONDAY SECURITY TIPS

INFORMATION PROVIDED BY NYS DIVISION OF CONSUMER PROTECTION

SHOP SAFELY ONLINE

Consumers should protect their personal identifiable information when making purchases online. It is imperative that consumers ensure they are conducting their transactions over a secure connection. Consumers can check this easily: Simply look at the URL of the website. If it begins with "https" instead of "http" it means the website is secured using an SSL Certificate and that communication with the webpage is encrypted. Consumers should also look for a small padlock icon in their browser's address bar, which also denotes that the website is secure.

BEWARE OF FAKE WEBSITES

As fraudsters continue to advance in sophistication to perpetuate a scam, fake websites resemble legitimate websites, with very credible-looking logos, pictures, and payment options. If the website is advertising extremely low prices, or discounts beyond 50 percent, consumers should be wary and diligently verify the legitimacy of the seller:

- Before shopping at an unknown website, consumers can verify the authenticity of the seller and website via an online search engine review. Consumers should look for a small padlock symbol in the browser's address bar to verify that the website is secure.
- Typos on the website are a red flag that the website may not be legitimate.
- Consumers should review the copyright date and domain creation date, as recently created websites are often a tell-tale sign of scam websites.
- Stick with retailers you know and trust and avoid shady third party seller websites from ads.
- Go directly to retailer websites rather than clicking on offers in ads or emails, and avoid offers in text message links.

ONLINE SECURITY

- Consumers should not use public computers or public Wi-Fi for any personal banking. Consumers should secure their computers, mobile devices and home Wi-Fi networks by ensuring that the operating systems and antivirus software are up to date with the latest security patches. They should also ensure their home Wi-Fi network has a strong password.
- Consumers should think twice before clicking on email links or pop-up advertisements. Unsolicited email offers or pop-up ads that appear to be from legitimate businesses may contain viruses or may be scams that sell knock-off products or never deliver purchased goods.

CHECK FOR FRAUDULENT TRANSACTIONS

- Keep an eye on your bank and credit card accounts online. Check in frequently and review the transactions.
- If you spot a suspicious transaction or anything unauthorized, call your bank and card issuer right away.

WATCH OUT FOR HOLIDAY SHOPPING SCAMS

- Brush up on common holiday phishing scammer tactics. Examples are Free Gift Card, Charity, Delivery, and Travel scams. Be wary of offers that are too good to be true.

FRIENDLY REMINDER

- Check with the retailers if they have an App on the Apple APP store or Google Play store if you plan on shopping with Apple or Android devices.
- Make sure your laptop or PC is updated with latest browser. Check if Chrome, Firefox or Edge is the latest version. In addition, check if the system has the latest antivirus/malware software and definitions.

NEW ROCHELLE BRANCH: 382 PELHAM ROAD, NEW ROCHELLE, NY 10805 • (914) 576-3200
IZETA DURAKOVIC - BRANCH MANAGER

RIDGEWOOD SAVINGS BANK
100 YEARS
Multiplying the Good for 100 Years

Visit **ridgewoodbank.com** or scan for additional security tips