Latah County Idaho
www.latahcert.us
contact@latahcert.us

OCTOBER 2023 NEWSLETTER

2023 CALENDAR

Holiday Break!!

Next meeting – January 2024

ONLINE SHOPPING and CYBERSECURITY

As we move into the holiday season and start cruising through our favorite online websites shopping for gifts, it's a good idea to review some simple guidelines to protect our pocketbooks, credit cards, computer devices, cell phones, and email from fraud and software disasters.

ONLINE SHOPPING

People used to have to go to stores to comparison shop, and clip paper coupons to get good deals. Now we're shopping, reading reviews, and checking for deals online from anywhere. With so many choices online, it can help to research products and companies and keep records of what we buy, as well as the promises a seller makes.

Learn About Sellers and Products

To check on unfamiliar products and companies, search online for the product or company name, plus the words "complaint" or "scam." See what other people are saying about their experience. Contact your state attorney general or local consumer protection agency to ask if there are complaints on file.

Read reviews with a critical eye!

Expert reviews from trusted websites are a good place to get information about what to buy and who to hire. Read customer reviews about a company or product from a wide variety of review and retailer sites, search engines, app stores, and social media platforms. Check several sources and consider where a review is posted, who did the review, and the reviewer's history. And don't rely on star ratings alone because some reviews and ratings are fake or misleading. Fake reviews can be positive or negative. Not all fake positive reviews are five stars. Some dishonest competitors place fake negative reviews. Also, its not always clear if a reviewer got something, like a free product, in exchange for writing a review. Some – but not all – websites will place a label or badge next to the review when they know that the reviewer got an incentive.

Comparison Shopping

To comparison shop for a product, make notes of the item's manufacturer or model number, plus details like size, color, or shipping fees. Collect information from product ads.

- Learn the cost of the product, including shipping, handling, delivery, taxes, or other fees.
- Read the terms of the advertised "deal." Do you have to buy unwanted products?
- Read the entire product description, including the fine print. Words like "refurbished," "vintage," or "close-out" could mean a product is in less-than perfect condition.
- See if a seller has a price-matching policy that guarantees it will match competitor's prices and match its own in-store price to its online prices.
- Find out if you can get a credit or refund if the item you buy today goes on sale next week.

Prepared by V. Lawrence, CERT

Delivery, Return, and Refund Policies

Read the seller's information about shipping and delivery. An FTC rule requires sellers to ship items as they promised in their ads. If a seller doesn't promise a time, it must ship your order within 30 days after it gets your name, address, and payment, or permission to charge your account. Many sites offer tracking options, so you can see exactly where your purchase is and an estimate when you'll get it. If you pay by credit card but don't get the item, you can dispute the charge!

Check the Seller's refund policies. The site should say whether you can return the item for a full refund. If you can return it, find out who pays the shipping cost of returns, how many days you have to return the item, and if you will have to pay restocking fees.

Check refund policies for sale items. If you buy things on sale, double-check the return policies. Sellers often have different refund and return policies for sale items, especially clearance merchandise.

Pay by Credit Card When Possible

Paying by credit card best protects you and your money in case of a scam, or if something else goes wrong. Make sure the websites where you enter payment information uses encryption to protect your information during your transaction. Look for https at the beginning of the URL (website address). The "s" after http means the site is encrypted – but doesn't mean it's a legitimate site.

If you pay by credit card and are charged twice for the same item, are billed for merchandise you never got, or get the wrong item or a defective item, you can dispute the charge or ask the credit card company to temporarily withhold payment while it investigates.

Never buy anything from online sellers that accept payment ONLY with gift cards, by wire transfers through companies like Western Union or MoneyGram, or with cryptocurrency. Payments you make that way are nearly impossible to trace and reverse.

Keep Records

When you buy something online, be sure to keep information about the following:

- ✓ the company name and website,
- ✓ what you ordered, the date, and what you paid,
- ✓ the seller's return policy,
- ✓ the company's promise to ship, and the date,
- ✓ all email, text, and other communications you have with the company, and
- ✓ your credit card or bank account statements that show how you paid.

Check the Site's Privacy Policy

The privacy policy should let you know what personal information the site is collecting, why its being collected, and how it'll be used. If you can't find a privacy policy, can't understand it, or don't like how the site will use your information, consider going to a different site.

If you have a problem when you shop online, try to work it out directly with the seller or site owner. If that doesn't work, report it to ReportFraud.ftc.gov, your state Attorney General, and your state's consumer protection agency.

USE STRONG PASSWORDS! Make your passwords long – at least 16 characters; complex – use upper and lowercase letters, numbers and symbols; and use a different password for each account.

TURN ON MULTIFACTOR AUTHENTICATION! It provides extra security by confirming your identity when logging into accounts, like entering a code texted to a phone or generated by an authenticator app.

RECOGNIZE PHISHING!

Common signs of a phish include urgent/alarming language, requests for personal or financial info, poor writing or misspellings, and incorrect email addresses or links. Delete it!

UPDATE YOUR SOFTWARE! Software updates protect your devices against the latest threats. Turn on automatic updates in your computer's settings menu.