Latah County Idaho

NOVEMBER 2021 NEWSLETTER

NEXT QUARTERLY MEETING: January 19 (Wednesday), 2022 at 7:00 pm at the Latah County Fairgrounds – Classroom.

CERT Curriculum Training – Unit 1 Disaster Preparedness: February 2 (Wednesday), 2022 at 6:30 pm at the Latah County Fairgrounds - Classroom

HOLIDAY TOPICS – CYBER SECURITY, COOKING AND FIRE SAFETY

The holidays are a special time of the year with time spent with family and friends, festive events, gifts, and good food. We also tend to be busy and under a bit of stress to make people happy and to provide the biggest and best parties, food, and gifts. This stress can cause us to take short cuts or do things fast at the last minute. The results of failing to pay attention can be disastrous including house fires, identity theft and food poisoning.

THE BASICS OF ONLINE SECURITY –

P. Gibson, Systems & Security Administrator

Staying safe online is a major concern in today's digital market. While it may seem like online finances and shopping are the most obvious targets for a cyber attack, it is important to remember that hackers constantly probe much more than just those. Any machine connected to the public internet receives an endless stream of exploit attempts. Modern technology only works because millions of systems all over the internet must be able to securely communicate with each other. Take Netflix for example, you can sign into Netflix using your Facebook account, which uses a portal connected to Google's reCAPTCHA service to protect against bot attacks so you can pay your bill using your bank debit card. This should not make you overly paranoid. Most of the time, these interactions go off without a hitch. The unfortunate reality, however, is that businesses MUST have an online presence now, and while businesses need to protect against countless security vulnerabilities when building and linking systems, a hacker only needs to find a single vulnerability to start his attack to take valuable information about you, the customer.

The truth is it is almost inevitable your sensitive personal information will be exposed at some point. Even if you do not use the internet at all, your subscription to Time magazine or your utility provider will have your information stored on systems which are connected to the internet. With this in mind, there are some important steps that will help keep you safe. These steps are outlined on the following page.

1. 

Phishy Emails: *Never* click on a link or download attachments from emails you do not know. A phishing email is an attempt to trick the person reading the email into taking action that would expose their information. Always check the email address on the message to make sure it is coming from the legitimate company listed in the mail. For example, an email from the United States Postal Service (USPS) would not be coming from US-PS.com. When you google USPS, you can see that the domain is USPS.com. If you have any doubts at all, delete the email.

2. 
Strong Passwords: Choose strong passwords. Despite what you have been told, it is better to have longer but easier to remember **pass*phrases***, instead of complex, hard to remember passwords. Avoid using commonly used passwords like "password" or "password123". Do not reuse passwords across websites. Pass*phrases* are just that, a phrase you use as a password. This means it is easy for a human to remember but hard for a computer to guess because they are so long. So, instead of using "ZD$&T53&K%-KbYuH", you can use "Don'tYouStepOnMyBlueSuedeShoes".

3. 

Your Debit Card Has a PIN for a Reason: Use multi-factor authentication (MFA) on any site that offers it. If they have the option to alert you to new login activity, enable that too. Always sign up using an email address that you have access to and can monitor. An example of MFA is that many banks now require you to enter an SMS (text message) code when logging into their site for the first time on a new computer. Personal Identification Numbers (PINs) are also used with many credit cards and online accounts. Someone would need to have your card (something you have), as well as the PIN (something you know) in order to access the account.

4. 
That Little Padlock in Your Browser's Address Bar: The padlock on your browser's address bar indicates that encryption is being used to securely send information on that website. Do not use websites that are not verified as secure in your browser. All modern browsers will alert you when the security certificate of a website cannot be verified. Remember, just because a site is verified as secure, does not mean it is not malicious, but a trusted site that has a certificate error is a red flag that someone may be trying to spoof the site.

5. 
Be Careful with Your Selfies and Social Media: Use caution when posting on social media. Be aware of details that bad guys can use such as posting vacation pictures while still out of town or personal information such as mother's maiden name, or names of pets. Additional detail called metadata is embedded in the photos. This information contains innocuous information like the type of camera used and the time the picture was taken, but also often contains GPS coordinates of where the picture was taken. You should also use caution when posting personal details. For example, many sites use security profiles to reset passwords. Common questions are things like "What is your mother's maiden name?", "What street did you grow up on?", "What was the make and model of the first car that you owned?", or "What is the name of your first pet?". These are details a diligent bad guy could discover by reviewing your social media and using to gain access to your accounts.

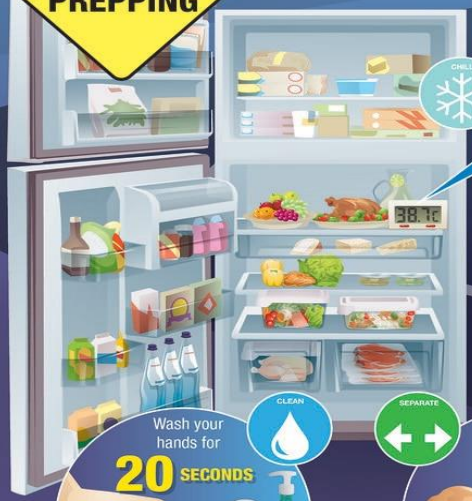
6. 
Your Computer Needs Updates: Computer updates might be frustrating, but they are a vital tool to keeping your system secure. As exploits are discovered and used, software manufactures become aware of them and fix (patch) them. These patches are part of what you get when you install updates from the manufacturer automatically. Keeping your devices such as your computer, phone, router, game console, and even some cars updated is important to staying safe. Be wary of downloading products that claim to manage updates for you, as they are often vectors for attack.

YOUR MAP TO A FOOD-SAFE HOLIDAY

Follow some simple food safety advice to keep you and your guests feeling festive this winter.

PROPER PREPPING

Just as you have a procedure for storing your holiday gifts when you get home, you should have a **system for storing your food.**



Make sure your fridge is set at or below **40 °F**

Chill perishable groceries within two hours of shopping

Store raw meats in a container or dish to prevent juices from leaking and set below ready-to-eat foods.

Wash your hands for **20 SECONDS** with warm water and soap!

Be sure to separate raw meat from ready-to-eat foods and dishes.

Don't forget: You need two thermometers.

One for the fridge to ensure food is stored at **40 °F.**

One for food, particularly meat, to ensure it's cooked to the right temperature.

WELCOME TO Roastville

Always use a food thermometer to check that different holiday meats have been cooked to the right internal temperature.

- GROUND BEEF 160 °F
- VEAL* 145 °F
- DUCK 165 °F
- PORK* 145 °F
- TURKEY 165 °F
- LAMB* 145 °F
- GOOSE 165 °F
- STEAK* 145 °F

YIELD

***Don't forget resting time!** Beef, veal, lamb, and pork should rest for **3 MINUTES** before carving or consuming.

HITTING THE ROAD

If you're bringing a dish to a get-together with coworkers, family or friends this holiday season, make sure you are transporting food safely.

KEEP COLD FOOD COLD

When transporting cold dishes, place items in a cooler with ice or gel packs to keep food at or below **40 °F**

KEEP HOT FOOD HOT

Keep hot foods at or above **140 °F** by wrapping dishes in insulation bags or towels and newspaper.

DANGER ZONE

DO NOT ENTER

Perishable food kept in the Danger Zone **(between 40 - 140 °F)** for longer than **2 hours** should be thrown out.

EXCEPTIONS to Danger Zone include ready-to-eat items like cookies, crackers, bread, whole fruit

USDA

Ad Council

For more food safety tips, go to **FoodSafety.gov**

Winter Holiday Safety

Winter holidays are a time for families and friends to get together. But that also means a greater risk for fire. Following a few simple tips will ensure a happy and fire-safe holiday season.

HOLIDAY DECORATING

- Be careful with holiday decorations. Choose decorations that are flame resistant or flame retardant.
- Keep lit candles away from decorations and other things that can burn.
- Some lights are only for indoor or outdoor use, but not both.
- Replace any string of lights with worn or broken cords or loose bulb connections. Read manufacturer's instructions for number of light strands to connect.
- Use clips, not nails, to hang lights so the cords do not get damaged.
- Keep decorations away from windows and doors.

HOLIDAY ENTERTAINING

- Test your smoke alarms and tell guests about your home fire escape plan.
- Keep children and pets away from lit candles.
- Keep matches and lighters up high in a locked cabinet.
- Stay in the kitchen when cooking on the stovetop.
- Ask smokers to smoke outside. Remind smokers to keep their smoking materials with them so young children do not touch them.
- Provide large, deep ashtrays for smokers. Wet cigarette butts with water before discarding.

Before Heading Out or to Bed

Blow out lit candles when you leave the room or go to bed. **Turn off** all light strings and decorations before leaving home or going to bed.

FACTS

- More than **one-third** of home decoration fires are started by candles.
- More than **two of every five** decoration fires happen because decorations are placed too close to a heat source.

NFPA NATIONAL FIRE PROTECTION ASSOCIATION
The leading information and knowledge resource on fire, electrical and related hazards

Your Logo