Help Protect Your Account from Fraud

Keeping your account safe is a shared responsibility. Learn how you can help.

Fraud occurs when criminals steal and use someone's confidential information without permission. Armed with stolen data, scammers can pretend to be you. All too often this causes huge personal and financial problems that are hard to fix. Confidential information includes data like your Social Security number, birth date, passwords, and debit or credit card details.

To learn more about what we do, click here or scan the code to read **Your Privacy and Security Matter**.

What We Do

We maintain high levels of security using data encryption, system firewalls, external network scans, and more. In addition, our debit card vendor constantly monitors transactions and watches for potential fraud.

What You Should Do

1. **Register your account online.** Setting up a username and password helps prevent unauthorized account access. Go to **HRAveba.org**. Click the **Login** button and select the type of account you have. Click the **Register** button and follow the instructions.

2. **Stay alert and monitor your account.** It's your responsibility to regularly check your account for accuracy and anything suspicious. You should frequently review your contact information, claims and debit card activity, spouse and dependent information, and direct deposit details to make sure nothing has changed or occurred without your authorization. You can do this online, from our mobile app, HRAgo®, and by reviewing your account statements.

3. **Sign up for e-communication and direct deposit.** With e-communication, you'll enjoy less mail clutter and better privacy protection. Direct deposit is faster, more convenient, and safer than waiting for paper check reimbursements in the mail. After logging in, click **My Profile** to check and update your **Account Preferences**.

If You Find a Problem

1. **Notify us as soon as you can.** Our customer care team is available Monday through Friday from 6:00 a.m. to 5:00 p.m. Pacific Time. We'll investigate and help you contain and resolve the issue. Generally, issues must be reported within 90 days of when they occurred.

2. **Immediately report debit card fraud by calling 1-877-591-4002.** Agents are available 24/7. Reporting debit card fraud is your responsibility. Be prepared to provide the date, amount, and merchant name for the transaction(s) in question. Our debit card vendor will investigate the problem, replace your card free of charge (if necessary), and usually make your account whole if fraud is reported within 60 days.

3. **Change your password.** You should immediately change your password if you notice suspicious activity, such as unauthorized claims, debit card transactions, account information changes, etc. Just give us a call or, from the online login screen, click **Forgot Password?** and follow the instructions.

General Security Tips

Follow these tips to help guard against cyber threats and scammers.

1. **Be Proactive**
   - **Use strong, unique passwords** of at least 15 characters. Consider using a reputable password management tool to store and generate unique credentials so you don't have to remember them.
   - **Enable multi-factor authentication** (MFA) whenever available. MFA makes it harder for thieves to log in as you, even if your password is stolen.
   - **Enable automatic software updates** for your operating system, browsers, and apps for the latest security protection.
   - **Monitor your account activity** regularly, including transactions, bank information changes, and address changes.
   - **Check your credit report** regularly for unauthorized activity.

2. **Be Careful**
   - **Never share your personal account information** or passwords with others, including family members and friends.
   - **Lock your electronic devices** with a PIN, biometric code, or password, and never leave them unattended in public.
   - **Avoid using public Wi-Fi networks** when accessing your accounts or sensitive data on your computer or mobile devices.

3. **Be Alert**
   - **Be skeptical of "urgent" requests**, generic greetings, or suspicious links in emails, text messages, and QR codes.
   - **Hang up on unknown callers** asking you to verity your confidential information.