Protect your benefits from fraud

Employee benefits accounts like HSAs, FSAs, and other plans contain funds and sensitive personal information, making them attractive targets for fraud. Learn how to spot warning signs and take steps to protect your benefits before fraud impacts you.

Why fraud prevention matters

From phishing attacks to unauthorized account access, fraud is a growing risk. If someone gains access to your account, they could:

- Spend your benefits dollars
- Change account details or reimbursement information
- Access your personal and health information

Resolving fraud can take time and may delay access to funds when you need them most.

Common fraud tactics

Fraudsters often use a mix of technology and manipulation. Stay alert to these common tactics used to target employee benefits:

Social engineering

Scammers create urgency or impersonate a trusted source. These messages may appear to come from HR, your manager, or a benefits provider and push you to act quickly.

Fake benefits portals and websites

Lookalike benefits or payment portals designed to capture login credentials or install malware – sometimes redirecting you to the real site after the damage is done.

Phishing, smishing, and vishing

- **Phishing:** Emails asking you to log in or verify information
- **Smishing:** Text messages requesting verification or account details
- **Vishing:** Phone calls attempting to collect personal or account information

Deceptive links

Links may look legitimate but redirect to fraudulent sites. Watch for:

- Slight misspellings or altered domains
- Numbers replacing letters
- Unexpected links related to enrollment, payroll, or claims

Spotting fraud and taking action

Best practices to reduce fraud risk

- **Monitor your accounts** regularly for unusual activity
- **Be cautious** with unexpected emails, calls, or messages – avoid clicking links and never share login credentials or verification codes
- **Use strong, unique passwords** and enable multi-factor authentication (MFA) whenever possible
- **Log in only through official websites** or trusted apps
- **Verify requests independently** using known, trusted contact information

What to do if something seems wrong

If you receive a suspicious message or notice unusual activity:

- Do not click links or download attachments
- Report it to your designated contact or benefits team
- Delete the message and block the sender
- If you interacted with a message, change your password immediately
- If you suspect fraudulent activity on your benefits card, report it as lost or stolen and submit a transaction dispute

Acting quickly can help limit the potential impact.

Red flags

- Urgent or threatening language (“act now” or “your account will be locked”)
- Requests for sensitive information (passwords, PINs, SSN, or bank details)
- Poor grammar, distorted logos, or unusual formatting
- Suspicious links or sender addresses that don’t match the provider

WEX will never send unsolicited messages asking for sensitive account information.