# TECH LINK

## Avoid Spring Scams

As we flip the calendar to spring, many of us are finishing up taxes and looking ahead to spring break or summer getaways. Stay alert and be wary of scams this spring by considering the following:

**Tax Scams**

- Be wary of any emails supposedly from the IRS (asking for personal information or credit card payment). Also know that the IRS does not send text messages.
- Don't be fooled by threats of any kind. The IRS will not threaten you with jail time or fines via phone, email or text.
- Protect your Social Security Number (SSN) and file for your tax return early. Once a scammer has your SSN, they have everything they need to create a tax return and have your tax refund sent to them. These scams often occur early on in tax season before most people have filed, so the scammer's tax return in your name and with your social security number gets filed first.
- Promises of a larger refund than you are entitled to - as with many scams, if it seems too good to be true, it likely is.

**Travel Scams from KnowBe4 Security**

If you're planning a trip soon, there are some things you should consider. For starters, is that dirt cheap flight to Tokyo too good to be true? Probably so, especially when the booking site also offers a boatload of other deals at shocking, unbeatable prices - who does that? A scam artist looking to take your money, that's who. For this reason, you need to learn how to sniff out these "too good to be true" offers. To help you out, here are some tips:

- **Go official:** Book a trip directly with an airline or hotel, or through a reputable agent/tour operator.
- **Do your research:** Do a thorough online search to ensure the company is legitimate. Are there very few pictures of the business' property, or unfavorable reviews? If they're suspect, other people may have posted their negative experience to warn others.
- **Stay safe online:** If sent a deal via social media or email, be very cautious and think before you click! The link may direct you to a malicious site. Make sure to pay special attention to the website name and domain. You may notice small changes in the name or domain – such as going from .com to .ru, which can direct you to a completely different company.
- **Pay safe:** Don't pay in cash, via bank transfer (MoneyWise, Western Union), or virtual currencies like Bitcoin. These payment methods are hard to trace and are non-refundable! Instead, pay with a credit card. Also, check that the website uses a padlock icon (https) on the address bar, indicating it's secure.
- **Check the small print:** Check that the website offers terms and conditions, refund policy, and a privacy policy.
- **Use your instincts:** If something sounds too good to be true, it probably is.
- **Report it:** Keep all of the evidence and report it to your local authorities right away.

Regardless of the time of year, you should always monitor your credit closely and consider locking your credit down until needed.