OREGON PUBLIC UNIVERSITIES
Retirement Plans

Fall 2021 Newsletter

2021 Virtual Benefit Fairs

We are getting so excited for the upcoming 2021 Benefit Fairs! We can't wait to connect with our current participants, as well as any new employees who may be interested in the Optional Retirement Plan (ORP) 401(a) plan, or the Tax-Deferred Investment (TDI) 403(b) plan. Due to the COVID-19 pandemic, the benefit officers of the seven public universities in Oregon agreed that it is too soon to see everybody in person. We are happy that they are keeping everyone's safety and health in mind during their planning processes. Therefore, the benefit fairs will be held virtually this year.

Please watch for upcoming email correspondence from your campus benefits office to determine the time and web address for your school's fair. Crystal Farset and Katy Hatfield from the Retirement Plans Management office will be available via Zoom drop-in rooms to answer any questions that you have concerning the ORP and TDI plans.

Crystal and Katy will be available for Zoom drop-ins on the following dates and times:

- October 4, 2021 from 1:00 P.M. to 3:00 P.M.
- October 5, 2021 from 8:00 A.M. to 10:00 A.M.
- October 6, 2021 from 2:00 P.M. to 4:00 P.M.
- October 7, 2021 from 11:00 A.M. to 1:00 P.M.
- October 8, 2021 from 1:00 P.M. to 3:00 P.M.

The Zoom link for access will be posted here on the day of each drop-in session.

We look forward to helping you with any questions that you may have. We hope to see you soon!

IN THIS ISSUE:

New Student Loan Forgiveness Benefit Brought to you by Savi and TIAA

The path to reducing your monthly student loan payment and working toward loan forgiveness could be getting much easier. That's because you have access to a robust solution that helps find the best federal repayment and forgiveness programs for your financial situation. And yes, the average student debt savings is $1,880 per year.[1]

Brought to you through TIAA and Savi, this tool not only helps strengthen your financial footing in the short-term, it also positions you for student loan forgiveness.

- Caps your payment based on your income and family size
- Frees up funds to direct towards other financial goals
- Removes the complexities of forgiveness and puts the process on auto-pilot for a small fee[2]

Join a free webinar to learn more

We're so excited to bring this opportunity to our employees. The service will be available to all university employees, as well as to their immediate family. Attend a 60-minute webinar and you'll see how easy it is to use Savi. You can also find out if you or a family member is eligible, hear about the costs to participate, understand how it works to reduce your monthly payment, and learn how to get started.

Register today!

- Friday, October 15, 2021 from 12:00 P.M. to 1:00 P.M. PDT

To get started today, visit tiaa.org/opurp/student today to calculate your savings. This calculation is available at no cost to you.

1. Between January 1, 2019 and December 31, 2019, based on Savi's internal measurements, Savi users saw average projected savings of $1,880 per year.

2. A portion of the fee may be shared with TIAA to offset costs to support the program. In addition, TIAA has a minority ownership interest in Savi.

Oregon Public Universities
Retirement Plans

Seven Great Reasons for Staying with the Oregon Public Universities Retirement Plans (OPURP) after retirement!

Congratulations! You have done what you needed to save money for your retirement. Now that you are getting ready to retire, you are probably thinking about the best way to invest your ORP and/or TDI accounts and how best to draw down the money you have been so diligent about saving. While you can roll your funds to an IRA, another option you may want to consider is to leave your money in your OPURP account(s), and here are some reasons you might want to do just that:

1. You do not have to take your money out of your ORP or TDI when you retire or terminate employment. In fact, you can leave your money in the Plan until it's time to take your Required Minimum Distribution (RMD).

2. You can consolidate other funds into your OPURP account. The plan accepts rollovers from any eligible plan, such as IRAs, the PERS IAP, and other eligible defined contribution plans from previous employers that you may have.

3. The OPURP offers low administrative fees that are competitively priced when compared to IRAs. Investment fees on the mutual funds are also very competitive.

4. The plans offer a variety of distribution options, including partial withdrawal, systematic withdrawal, specific dollar amounts, and monthly installments.

5. Each vendor offers a variety of mutual funds to choose from, including low-cost target date funds. Fidelity also offers a self-directed brokerage account which gives you access to hundreds of mutual funds in the TDI; in the ORP you also have access to stock and bond options. AIG and TIAA also offer annuities.

6. Investment oversight comes from the OPURP Investment Committee and outside investment consulting firm, Callan LLC. The funds are reviewed and monitored on a quarterly basis.

7. You still have access to the vendor representatives who you can meet with one-on-one to discuss investments and draw down options.

Contact OPURP with any questions you may have at OPURP@uoregon.edu.

4 tips to protect against identity theft

Safeguard your sensitive information and financial accounts by taking these steps.

Key takeaways

- Be wary of emails, phone calls, or texts that ask you to supply information like a password or personal information.
- Be aware of the fact that your phone can be hacked.
- Take steps to secure financial accounts with the highest level of security offered—and then monitor them for any unauthorized activity.
- Keep computers and mobile devices updated and secured with strong passwords.

Identity theft can be scary but there is good news. You can protect yourself, in most cases, by being aware of the threat and following certain practices for safeguarding your information.

1. Don't take the phishing bait

Phishing is a technique used by criminals to trick victims into providing personal information that can be used for identity theft. Most phishing attempts are carried out by email, text messages, or phone.

- Ignore deals, freebies, and awards that sound too good to be true. Disregard offers that appear to come from unusual foreign contacts, as well as requests from strangers for help.
- Ignore phone calls, emails, or texts that appear to be from the IRS. The agency will not contact you by phone, email, text message, or social media to request personal or financial information.
- Be suspicious of anyone requesting your Social Security number, date of birth, financial account number, PIN, email, or passwords—especially if there is a request to verify your information when you were not expecting it.
- Never click a link or download an attachment inside an unexpected email. If the email claims to be from a company you do business with, don't log in from a link in the email message—go to the company's website and log in to your account from there.
- Never provide personal information over the phone to an unsolicited caller. If you think the call might be a legitimate request from a company you do business with, hang up, and call the company directly.

2. Protect your phone service

Your phone has become an important part of security protocol and is the "master key" to accessing online accounts and information.

Criminals and scam artists are actively using stolen identity information to port your mobile phone number or forward your phone calls and text messages. They do this by calling phone service providers. If you use Voice over IP (VoIP) phones, then your voice phone portal accounts are also at risk.

Cyber criminals do this to steal your 2-factor authentication codes and text messages to get into your financial institution accounts.

- Learn signs that your phone may be hacked. If you notice your mobile phone showing "no service" or "emergency calls only," or you stop receiving phone calls and text messages even after you restart your phone, contact your mobile company to see if your account has been compromised.
- Ask your telecom provider about ways to better secure your account, especially verifying your identity with a PIN or 2-factor authentication to make changes, route phone calls, forward phone messages, or port your phone number.
- Secure your online phone and internet service provider account where you pay bills and manage settings. Use a separate and strong password for such accounts and enable 2-factor authentication on these accounts.

3. Monitor and secure your accounts

Many companies, including Fidelity, go to great lengths to safeguard customers' information and provide security tools. For instance, Fidelity offers 2-factor authentication, designed to prevent someone from accessing your account, even if they have your password.

Here are a few actions you can take to reinforce those safeguards.

- Choose passwords that can't be guessed easily. Use different passwords for different websites and change them regularly.
- Sign up for 2-factor authentication at your financial institutions and email service providers to protect all your online accounts.
- Make sure your financial institutions have up-to-date contact information for you, especially your mobile number. Your financial institutions use this information to protect your accounts and to contact you when suspicious activity is detected.
- Sign up for automated alerts of suspicious account activity wherever offered. Fidelity automatically alerts you by email and text messages of certain suspicious activity. Do not ignore these security alerts when they are received.
- Check your credit report regularly. The 3 major agencies—Equifax, Experian, and TransUnion—are required by law to provide you with a free copy of your credit report once every 12 months, which means you can check your report for free 3 times throughout the year.

4. Secure your mobile devices and personal computers

Any device you use that is connected to the internet can become a mechanism of attack by cyber-criminals.

Hackers can get in through newly discovered security holes in these devices and systems.

- Change any default passwords when setting up your devices.
- Apply updates and patches as soon as the system maker releases them.
- Don't download mobile apps and games that you do not trust. Some mobile apps have been found to contain hidden malicious software. Use your best judgment before using a brand-new app from an unknown company and read reviews before downloading.
- Run antivirus software on your computers and ensure that your mobile devices have the most recent security updates and patches.

Take security seriously

Protecting your information and online accounts can help avoid the hassle and heartache of ID theft. Take advantage of all security measures offered and use strong passwords—remember the best way to prevent identity theft is with a strong defense.

Understanding the Differences Between the Oregon Public Universities 403(b) Tax-Deferred Investment Plan, and the Oregon Savings Growth 457(b) Plan

The Oregon Public Universities Retirement Plan (OPURP) office regularly receives questions from employees who are interested in investing in the Tax-Deferred Investment 403(b) plan and/or the Oregon Savings Growth 457(b) plan.

There are multiple facets to each plan, which makes them unique from one another. Our office has created a comparison sheet that indicates the differences and similarities of each plan based on plan features.

Oregon Public Universities Retirement Plans

Comparison of the Oregon Public Universities Retirement Plan TDI 403(b) Plan and the Oregon Savings Growth Plan (OSGP) 457(b) Plan

Feature	403(b) – OPURP TDI	457(b) - OSGP
IRS Annual Contribution Limits	2021 Limits $19,500 $6,500 Additional for age 50 and up.	2021 Limits $19,500 $6,500 Additional for age 50 and up.
Transfers between Fidelity, TIAA and AIG	Transfers allowed from AIG to either Fidelity or TIAA; and allowed between TIAA and Fidelity.	Not allowed.
Rollovers	Allowed from eligible plans such as 401(a), 457(b), 403(b) and traditional IRAs.	Allowed from eligible plans such as 401(a), 457(b), 403(b) and traditional IRAs.
Loans	Two loans maximum. Loans are not allowed if you have a defaulted loan.	One loan maximum. Must wait one year after paying off loan to get another.
Emergency Distributions	Yes, hardship allowed as defined by Plan.	Yes, unforeseeable emergencies allowed as defined by Plan.
Catch-Up Options • **Age 50 and over** • **3-year catch-up**	 Yes No	 Yes Yes
Distributable Events	Age 59 ½, severance from service, disability, or retirement. Age 72 required minimum distributions.	Age 72 required minimum distributions, severance from service, retirement, or disability. De Minimis withdrawals.
Roth Contributions	Yes	Yes
Distribution Options • **Lump Sum** • **Partial Lump Sum** • **Installment** • **Annuity Payments**	 Yes Yes Yes Yes	 Yes Yes Yes No
Expenses and Fees Paid by Participants:	Administrative and Record Keeping fees. Investment Fees on funds. Loan fees differ by Vendor.	Administrative and Record Keeping Fees. Investment Fees on funds $75 loan fee.
Taxability	Pre-tax contributions and earnings are taxable at the time of distribution. No taxes on Roth contributions or earnings.	Pre-tax contributions and earnings are taxable at the time of distribution. No taxes on Roth contributions or earnings.
Early withdrawal penalties	10% tax penalty if under age 59 ½	No.
Funds	Variety of mutual funds and annuities. Self-directed brokerage account at Fidelity.	Variety of mutual funds, stable value, and self-directed brokerage account.

Please note that you can contribute to both the 403(b) plan OPURP and the 457(b) plan with OSGP. If your resources allow, you can maximize your contributions to both plans and contribute a total of $39,000 per year, or for those age 50 and older, an additional $13,000 can be contributed, for a total of $52,000. OPURP has oversight of the 403(b) plan and its investments. OSGP is administered by PERS.

Let's Talk About Cyber Security and Different Ways TIAA is Helping Keep Your Account Safe

At TIAA, your security is a top priority, and we combine technology, people and process to protect our customers. The use of multi factor authentication provides an additional layer of security by requiring an additional verification, such as a one-time PIN or biometric recognition.

You can easily enable the use of a one-time PIN, biometrics, voice identification and security questions on the Security Preferences page in your TIAA Account Profile.

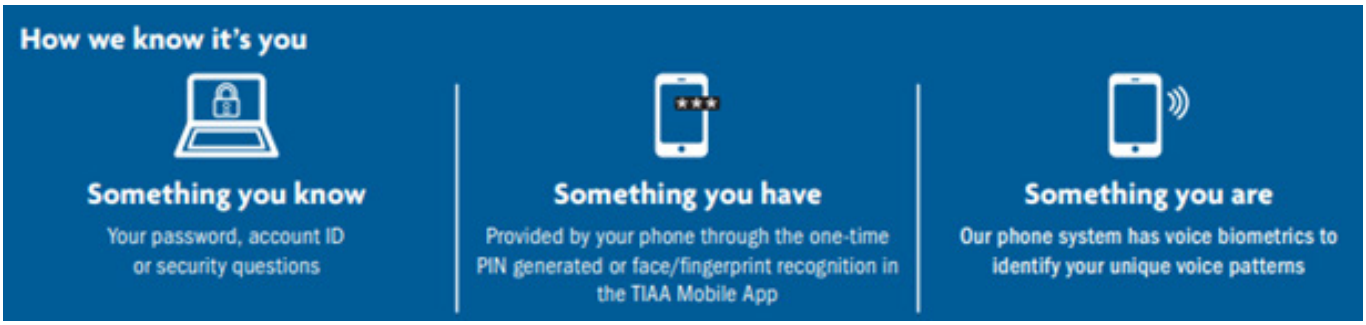
To do this, log into your TIAA account.

1. On the top, right-hand corner of the screen, click "Profile"

2. A page will then load with different categories listed. Click on the option titled "Security Preferences"

3. A new page will then load, which will allow you to update one or multiple sections

4. Once you have made your desired changes, click "Save Changes"



How TIAA protects your accounts

We go to great lengths to protect your TIAA account from unauthorized access.

1. Encryption:

We encrypt sensitive communications sent outside TIAA to protect your data.

2. Secure Login

You receive enhanced login security through risk-based and opt-in authentication via text messages.

3. Online experience

You get a secure online experience whenever you're logged in

4. Monitoring

We keep the site secure through regular audits and security patches.

Common questions that come up around cyber-security:

What options are there for multi factor authentication (MFA)/two-step identity verification on TIAA.org?

- TIAA applies an adaptive risk-based, multi factor authentication (MFA) approach. We also provide all customers the option of setting their security preferences to default on MFA for all their logins, which adds an additional layer of security and provides a consistent login experience, regardless of what devices are used to connect to us.
- Beyond login, TIAA may also require additional verification during important account changes and/or financial transactions, whether they are made online or over the phone.
- TIAA also offers voice biometric authentication. Voice biometrics protects you in our telephone servicing. When you call, you can simply use your voice to authenticate and by enrolling, we provide you with the strongest level of security for our telephone services.
- Depending on your mobile device, we offer the convenience of using face and/or finger print recognition using the TIAA Mobile App, to further enhance security.

What is voice biometric authentication?

Voice biometric data is used solely to verify your identity as a TIAA customer so you can access your account.

- We will not disclose your biometric data to any third party, unless required by law or with your consent.
- You may opt-out or deactivate your consent to use your voice print at any time.
- We protect your biometric data with operational, administrative, technical and physical security safeguards in accordance with applicable law.
- Only one voice print is allowed per account and is reserved for the account owner. If you are ever unable to complete enrollment, your call will be directed to a TIAA representative for additional assistance.

TIAA Protects your Personal Information

We combine technology, people, and processes to protect customers and their personal information Read our privacy notice for additional details.

TIAA will always

- Protect your confidentiality
- Defend against anticipated threats
- Protect against unauthorized access
- Adhere to all state and federal regulations

Report something suspicious by calling us at 800-842-2252. We're here every weekday from 8 a.m. to 10 p.m. EST.

Cyber-Crimes: Avoid Phishing and Spear-Phishing

Phishing and spear-phishing are an attempt to acquire information, such as usernames, passwords, and company data, by masquerading as a trustworthy entity via email. With phishing, the cyber-criminal is directing an email at a large group of people. Phishing is the top entry point for cyber-attacks[1] with 92.4% of malware delivered by email via hyperlinks or downloadable content[2]. With spear-phishing, the cyber-criminal is targeting a specific targeted individual. 71% of targeted attacks include spear-phishing[1].

Be on the look-out for emails, calls, and text messages to have these characteristics[3]:

- Grammar and spelling errors
- Requests to click on links or open attachments
- Sense of urgency
- Appeal to human greed and fear
- Request for sensitive data

If you ever suspect an email, call, or text message to be phishing or spear-phishing, DO NOT click any links or open attachments. Criminals take the time to understand your relationships, activities, interests and travel or purchasing plans in order to gain your trust. They also gather information from social media, websites and LinkedIn accounts, making it easy to send you targeted malware.

Stay safe online:

- Verify the sender's email address: criminals use spoofed email addresses, usually one or two letters off from a company's true domain name.
- Do not enter your username and password into a web page from a clicked link.
- Keep your browser, plugins, and security software up to date.
- Verify the URL is legitimate by checking domain property.
- Do not trust phone numbers found in suspicious email messages.
- Use saved bookmarks to navigate directly to correct websites.

[1]Symantec
[2]CSO Online
[3]Cofense

Cyber Safety Tips for Parents

Do you parent or interact with a pre-teen or teen? 97% of teens report that they use social media daily[4]. It is important to have an open dialogue with your children on how they interact online, including knowing which games they play and how they are involved in social media.

Help your children stay secure in cyberspace with these tips:

- Enable parental controls for device and individual apps.
- Discuss what personal information not to discuss with online "friends."
- Monitor phone usage, including implementing limits on app purchases.
- Check for geolocation settings: A GPS-enabled smartphone can reveal your child's location through online posts and uploaded photos.
- Read Terms & Conditions that give away Personal Identifiable Information (PII).
- Search your kids' images on Google to see if they've been replicated on other sites or otherwise used without your permission.
- Keep devices out of the bedroom at night by having charging stations in the family room.

[4]Pew Internet Research 2018 (Teens age 13-17)

Could you be a target for cybercrime?

Understanding the potential threats can help keep your online accounts safe.

Key takeaways

- Understanding the many forms of cybercrime may allow you to better defend yourself.
- Use 2-factor authentication for all online financial accounts.
- Maintain updated industry-standard operating systems and software.
- Do not use public Wi-Fi for your finances or other sensitive items.

You've likely spent a good deal of time thinking about investment risk. But have you stopped to think about more personal security issues, such as the safety of your online financial transactions and information stored on your computers? While most people recognize that online fraud or cybercrime is a potential threat, few know how or why they may be at risk. Cybercrime can take many forms and understanding who the enemies are and how they commit crimes may allow you to better defend yourself.

The "Bad Guy"

Economic cybercriminals pose the greatest online risk to your family's personal financial data and assets. Make no mistake, many of these thieves are highly skilled and sophisticated. They may be individuals or coordinated groups that use technology to steal. For most of us, cybercrime can best be described as an extension of traditional criminal activity focused on personal financial data and monetary theft.

How do cybercriminals operate?

Indiscriminate targeting

In some cases, cybercriminals cast a wide net with "phishing" scams, among others, and hope the sheer quantity of potential victims will yield sufficient economic benefit (see "The makings of a cybercrime," below, for more details on how cybercriminals attack).

Specific victim targeting

A growing and more concerning trend is the specific targeting of high-net-worth individuals. In many of these cases, criminals spend a great deal of time and effort identifying a worthwhile target and then developing a victim profile based on public and private information—such as property records, credit information obtained via hacking, and posted details on social networks—with the goal of stealing assets from financial accounts. Although the actual criminal act can take several forms, the basic steps are often similar. Below is a relatively common scenario:

- **Step 1:** The thief sends an email with a link or attachment to the victim that appears to come from a known party. The targeted victim then clicks the link or attachment, which includes malicious software (malware) that infects the victim's computer.
- **Step 2:** The thief uses installed malware to steal login credentials to the victim's financial accounts or to remotely control the victim's computer. This will generally allow the thief to log in as the victim.
- **Step 3:** With access to accounts, the thief changes the victim's profile at the financial institution and/or impersonates the victim and moves money to criminal accounts at a different institution.

That's the bad news. The good news is that with some simple steps, you can improve your defenses and reduce your vulnerability to this type of crime.

How do I keep my online accounts safe?

1. Protect your online access with unique user IDs, passwords, and 2-factor authentication for each site

Treat your computers and websites as you would your front door—restrict access and use tough security measures. Passwords are the keys to your online financial information. If cybercriminals find them, they can unlock the doors to your bank accounts, investment accounts, and your personal information. Unfortunately, a significant amount of malicious software trolls the internet looking specifically for account credentials (IDs and passwords). With an inadvertent click on what appears to be a legitimate link, or the opening of an attachment designed to look legitimate, this software can be loaded on your machine and be ready to take your "keys."

Go for 2

Adding an additional layer of security when you access your accounts, called 2-factor authentication, is a strong defense against most common attacks. Fidelity and many other financial firms now offer 2-factor authentication. It requires you to enter a unique security code, randomly generated and sent to your phone or other mobile device, in addition to your standard login ID and password. While not completely foolproof, 2-factor authentication raises the bar for cyberattackers trying to access your accounts. Consider enabling 2-factor authentication for nonfinancial sites, such as your mobile phone billing sites (e.g., AT&T, Verizon, T-Mobile, Xfinity) and email sites (e.g., Google Gmail, Apple, Microsoft, Yahoo, Hotmail).

Make sure your financial sites and email providers have your mobile phone number as it is generally used to secure your online access.

Go long and stay strong

You've probably heard this before, but it bears repeating: Never use names, birth dates, Social Security numbers, or any personally identifiable information as your login ID and password. Use a different password for every application and website. Why? The dangers of password reuse. Every year there are data breaches and more sets of credentials (user IDs and passwords) leaked onto the internet. It is common practice these days for criminals to collect these credential dumps and try these login IDs and passwords at financial sites, email providers, mobile phone providers, social media sites, and others. If a Fidelity customer were to use the same password here that they used on another website, and that other account was breached, their Fidelity account could be at risk.

What constitutes a good password? Long (10 or more characters), and complex (combination of special letters and numbers) help make passwords more unique. A string of unrelated words with numbers and special characters in between is best. Stay away from single dictionary words or common combinations of words.

Go with a password manager

These days, most of us have dozens of passwords covering multiple devices and everything from email accounts, telecom billing, and subscription services, to social media, online shopping, and banking. Remembering all these passwords, and changing them frequently, just isn't sustainable and as a result we have a tendency to reuse the same password everywhere. This is the worst practice though. Fortunately, there's an app for that. Password manager apps generate and store all your passwords in a secure environment. They'll even auto-fill login information for stored sites. Many now sync your passwords across all your devices and automatically generate new ones on a regular schedule. The cost of state-of-the-art password managers is negligible—especially when compared with the convenience and security they provide.

2. Secure devices and software, keep them up to date, and perform regular backups

One of the smartest things you can do to keep your financial information safe is to use modern and up-to-date, operating systems. Software makers have teams of cybersecurity specialists dedicated to fixing vulnerabilities in their current systems, and they are always on the lookout for new ways cybercriminals can hack into their products to access users' computer files or install malicious software.

Updating your systems is easier than it used to be

Today, most operating systems let you set your preferences to automatically install updates and patches as soon as they are available. That goes for software too, including antivirus protection. Don't forget to update your mobile phones and tablets, and the apps installed on them. You can set update preferences to do this automatically on your devices.

You can never have too much backup

Backing up your data is good system hygiene. It prevents your information from being lost forever and immunizes you from ransomware attacks. In this increasingly common scheme, criminals lure you into clicking an email link that downloads malware and blocks your access to the computer. The perpetrators can hold your hard drive hostage, demanding a hefty ransom to unblock it. If your system data is backed up elsewhere, it eliminates any leverage the scammers have, neutralizing their threats.

Backups are most effective when done frequently. Savvy users employ redundant methods—typically a USB-connected external storage device in tandem with an encrypted cloud-based service. External storage offers more immediate data retrieval, while cloud-based services can store much more data. Also, in the event of a flood or fire, both the computer and external storage device may be lost, but offsite backups to a cloud-based service would be safe.
Don't forget to include mobile devices in regular backups. This can be done via a cloud-based service, but a full backup may require connecting to a computer. By syncing up your photos and home movies to your computer, they will then be included in regularly scheduled backups, keeping them secure.

3. Avoid accessing financial accounts or e-commerce sites through links in email

Cybercriminals are getting smarter about making their phishy emails look legitimate. These emails mimic those of financial institutions, complete with logos and convincing signature lines. Sometimes, the criminals impersonate emails appearing to come from friends, family members, or professional contacts you trust. Searching Google and social media sites makes it easy to personalize these emails with your name and subject lines like "Your recent transaction with us." All of this is designed to lower your guard, so you'll be more apt to click a link to a fraudulent version of your financial website. This allows the scammers to download malicious software onto your computer or gain access to your passwords and usernames.

When it comes to security, emails cannot be trusted

Avoid clicking links in your emails to access your financial sites online, no matter how compelling the language in the email appears. Instead, go directly to your provider's website by using a link you've saved in your "Favorites" menu. That way, you'll be sure you arrive at a legitimate website. Always look for the "https" prefix in the site's address. This indicates that the connection to the site is encrypted to protect your sensitive data from prying eyes. And if there is an ask by email to send money, always call your contact by phone to confirm the request along with transfer details even if you were expecting the ask.

4. Always access your accounts from a secure Wi-Fi location

Your home Wi-Fi network comes with built-in security. Your network provider supplies you with a wireless router ID and password, but these are default settings. Cybercriminals know the defaults for major network providers. If you're using these settings, your "secure" home Wi-Fi network may not be as secure as you think.
Home networks now connect computers and smartphones to thermostats, TVs, refrigerators, and residential security systems. Each device is a potential weak spot in your Wi-Fi network. As your home becomes more dependent on the internet, so does your exposure to a network breach.
When setting up your home network, consider changing the default Wi-Fi network name and passwords.

Beware of public Wi-Fi

Everyone loves free Wi-Fi, but unsecured public wireless access points are easy to intercept, providing an opportunity for attackers to snoop on your online activity. A safer alternative is to use only secure Wi-Fi networks. If you use your laptop or mobile devices while traveling, purchase a subscription to a paid hotspot provider in which the networks are password protected and have additional levels of security.

5. Consider using a dedicated device for online banking

One of the best ways to secure your online financial information is to dedicate one device exclusively for banking and financial use. Many cyberattacks come from malware installed while you are web surfing and reading emails. Eliminating those activities from a dedicated banking computer goes a long way toward keeping your financial information out of harm's way.

Help us help you

A dedicated banking device also helps financial institutions keep your accounts secure. Most, including Fidelity, monitor client accounts for fraudulent logins from unauthorized computers and will alert you if there is suspicious activity in your account. When Fidelity surveyed client login patterns, we found many users logging in from

multiple devices. One or two were common, but some clients routinely logged in from a seemingly random assortment of systems, making it difficult for an institution to distinguish a legitimate login from a fraudulent one. By using one device for all transactions, an illegitimate login stands out, and the institution will be able to move quickly to alert you and secure your account.

6. Understand your computing environment and consider whether you need help

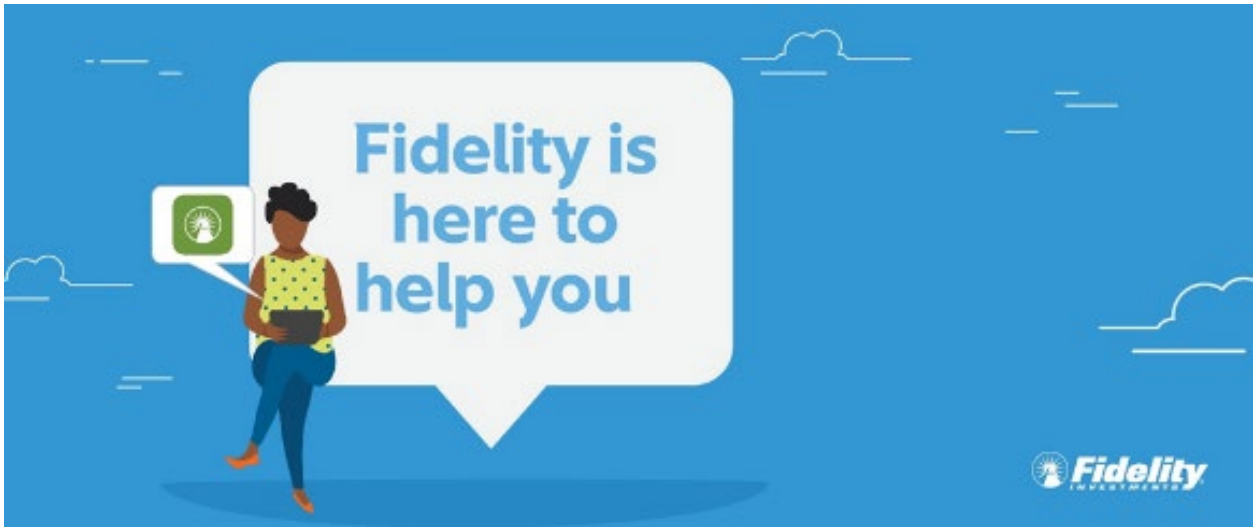
If you have a complex computing environment, a comprehensive cyber-risk assessment may be an appropriate step in protecting your personal information. Individuals with complicated online footprints may want to consider implementing additional systems (e.g., intrusion prevention and detection, firewalls).
Because cyber threats evolve almost as fast as technology itself, consider retaining a firm to provide ongoing system surveillance, support, and maintenance. These services include everything from monitoring your home internet traffic and blocking outside threats, to educating family members about smart social media practices, safe web surfing and e-commerce protocols.

A good risk assessment will be specific to each person and should consider questions like:

- How many computers, mobile devices, tablets, TVs, home security systems, and appliances are connected to your home Wi-Fi network?
- Are they shared across personal and business or home office use?
- Do non-family members regularly in your home have access to your Wi-Fi network or computing devices?
- What backup procedures are in place for each device?
- Are you or other household members active on social media like Facebook, Twitter, or Pinterest?

Conclusion

No one wants to spend time thinking about all the bad things that can happen, but it's important to understand potential threats to your assets and take measures to eliminate them. When it comes to protecting your financial accounts from cyber threats, practicing good system hygiene and making a few changes in your online habits will significantly improve your security. You play a key role in helping Fidelity detect fraud by maintaining a general awareness of your accounts, including staying alert to notifications regarding password resets, money transfers and account changes, and periodically logging in and checking for unusual transactions and activity.
Fidelity uses sophisticated security measures to protect our customers. We also make many additional security tools available for customers to utilize, including 2-factor authentication and transaction alerts. Of course, we also provide a Customer Protection Guarantee for fraudulent activity. Make sure to visit Fidelity's online customer security site to explore some of these features and learn more about what Fidelity is doing to help keep your assets safe.



Virtual and Phone-Based Consultations

At Fidelity, we're here to help you give attention to your own future; we are committed to helping you make sure you're on track toward a future that's unique to you. Meet with us one-on-one and you'll be able to tap into the education, resources, and support that only a trusted partner can provide. Plus, consultations are free to you as an employee benefit.

Justin Blatny and Ronald Elia will be offering virtual and phone-based one-on-one consultations to all Oregon Public University employees and they are ready to help you address many questions, including:

- ✓ Am I investing properly?
- ✓ Am I on track with my retirement savings?
- ✓ How do I bring my retirement savings together?
- ✓ How do I turn retirement savings into ongoing, steady income?

Click HERE to view a schedule of dates and times when Justin and Ronald will be available for consultations. Be sure to type "Oregon Public Universities" as your employer's name, not your specific campus name.

Justin and Ronald are licensed professionals, experienced in helping people plan for their financial futures. You can meet with them whenever you want and can ask them anything. Really!

Meet with a TIAA Financial Consultant

Schedule a virtual or by-phone appointment with a TIAA financial consultant to discuss steps to take to feel more financially confident and secure.

Schedule easily on your Oregon Public Universities TIAA microsite or call us. Contact information is below:

https://www.tiaa.org/public/tcm/opurp

Schedule a one-on-one session with a TIAA financial consultant by calling (800)732-8353 weekdays from 5:00 a.m. to 5:00 p.m. (PST)

CONTACT US

OREGON PUBLIC UNIVERSITIES RETIREMENT PLANS (OPURP)

MAIL:
6226 UNIVERSITY OF OREGON
EUGENE, OR 97403-6226

TELEPHONE:
(541)346-5784

FAX:
(541)346-5783

EMAIL:
OPURP@UOREGON.EDU

WEB:
WWW.OPURP.ORG