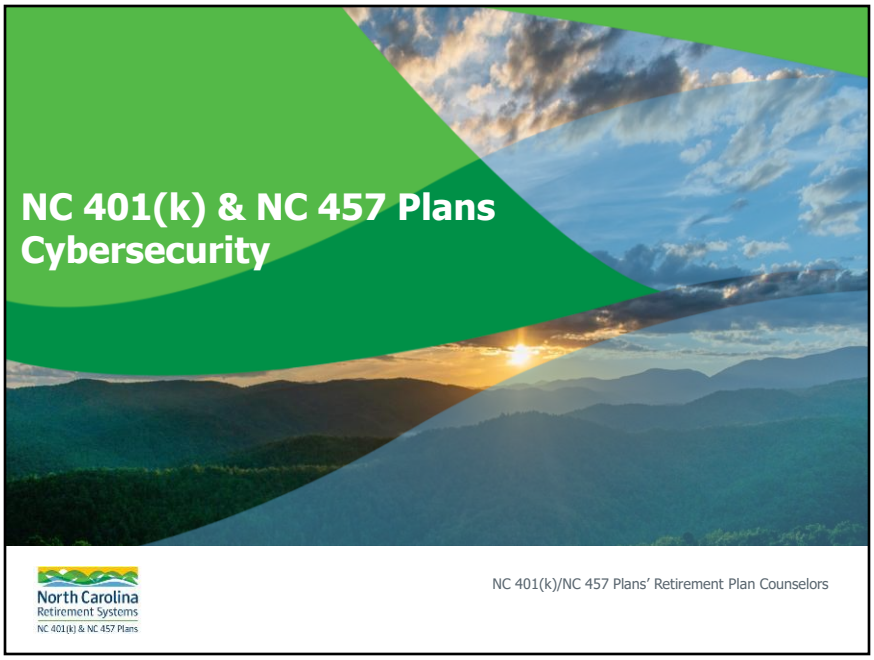


Speaker Text:

Hello and welcome to our presentation today.

My name is **[speaker]** and I'm an NC 401(k) and NC 457 Plans' Retirement Plan Counselor. **[Give a little information about who you are and what you do]**

Today we will talk about…

- Plan features
- Types of Plan contributions
- Accessing and consolidating savings
- Cybersecurity
- Resources



[read slide]



[read slide]

NC 401(k) and NC 457 Plan Features

	NC 401(k) Plan	NC 457 Plan
State-sponsored	Yes	Yes
Eligibility	Full-time, temporary or part-time employees[1]	Full-time, temporary or part-time employees[2]
Employer contributions[3]	Possibly, check with your Employer	Possibly, check with your Employer
Contribution types	Pre-tax, Roth	Pre-tax, Roth
No minimum	Yes	Yes
Contribution flexibility	Yes – changes anytime	Yes – changes anytime
Vesting	100%	100%
Rollovers	Yes	Yes
Age 50+ catch-up	Yes	Yes
Three-year catch-up provision	No	Yes
GoalMaker®	Yes	Yes
Investment oversight by DST and Board	Yes	Yes
Withdrawals while working	At or after age 59½	At or after age 59½
Loans/hardship withdrawals	Yes	Yes
Purchase of service credits	Yes	Yes
Multiple distribution options	Yes	Yes
Transfer benefit	Yes	Yes
Early withdrawal tax penalty	Possibly, depending upon age at separation from service and withdrawal method	Never incur 10% early withdrawal penalty regardless of age

[1] Also eligible: elected or appointed officials, rehired retired employees and contributing members to one of the North Carolina Retirement Systems, including TSERS, LGERS, LRS and CJRS.
[2] Also eligible: elected or appointed officials and rehired retired employees. Employer must offer the Plan.
[3] Employer contributions are discretionary and reduce the amount that an employee can contribute.

Speaker Text:

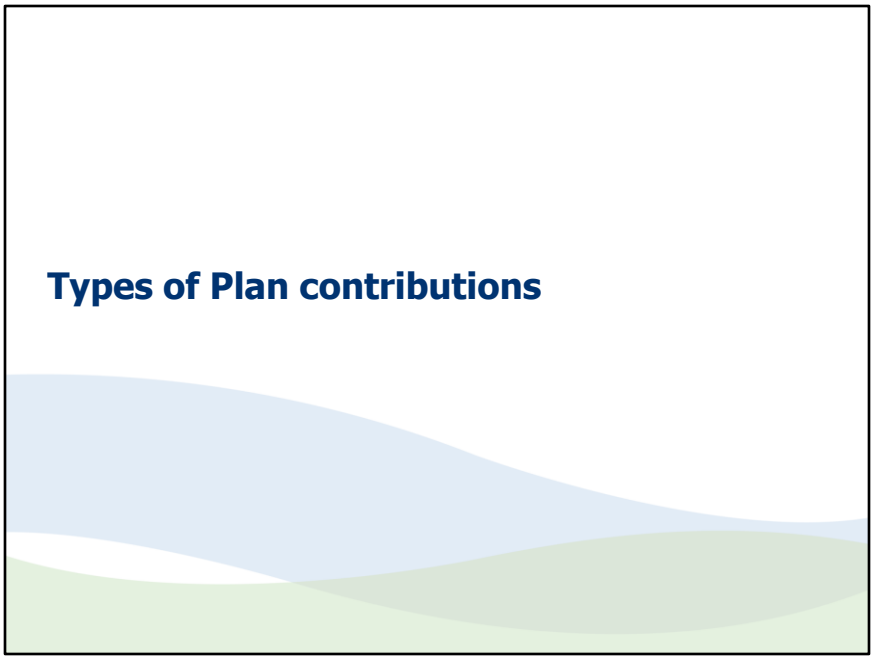
This chart gives you a side-by-side comparison of many of the NC 401(k) and NC 457 Plan features.

Differences between the NC 401(k) and NC 457 Plans

	NC 401(k) Plan	NC 457 Plan
Three-year catch-up provision	No	Yes
Loans/hardship withdrawals	Yes, under seven conditions, as approved by IRS	Yes, under four conditions, as approved by IRS
Early withdrawal tax penalty	Possibly, depending upon age, years worked for some, and withdrawal method	No early withdrawal penalty, regardless of age at separation of service

[1] LEOs and certain local pensions are also eligible.

And this chart shows you the *differences* between the two plans.



[read slide]

Less impact on your pay with pre-tax contributions



	Not Contributing $	Contributing $
Nick's salary per month	$3,000	$3,000
Voluntary contribution	**$0**	**$90**
Taxable income	3,000	2,910
Taxes (NC state & federal income tax)	923	895
Nick's take-home pay	**$2,077**	$2,015

Paycheck is only **$62 less**

For illustrative purposes only. Assumes 5.75% NC State Tax, single filing status, one allowance and a federal income bracket of 25%. Retirement plan distributions will be taxed upon withdrawal. Amounts withdrawn are subject to income taxes. This information has been provided for your benefit and is not intended or designed to be tax advice. Neither Empower Retirement, LLC nor any of its representatives, may give legal or tax advice.

Speaker Text:

One of the major benefits of investing in an employer-sponsored retirement plan is that your contributions are tax deferred. This means that each dollar you save is one less dollar that your employer reports to the IRS as income. This lowers your current federal tax liability and, as a result, does not impact your pay as much as you might think.

Let's take a look at an example. Here's how Nick's paycheck looks before he starts saving in the Plan. What happens to his paycheck after he starts saving 3 percent of his pay? His take-home pay is only $62 *less* than before he started saving. That's the power of tax-deferred investing.

Save on current taxes with pre-tax contributions



Contribution Amount	Estimated Tax Advantage	Reduction in Take-Home Pay
$25	$ 7.69	$ 17.31
$35	$ 10.76	$ 24.24
$50	$ 15.38	$ 34.62
$75	$ 23.06	$ 51.94
$100	$ 30.75	$ 69.25
$150	$ 46.13	$ 103.87
$200	$ 61.50	$ 138.50
$300	$ 92.25	$ 207.75
$500	$ 153.75	$ 346.25

For illustrative purposes only. Assumes 5.75% NC State Tax, single filing status, one allowance and a federal income bracket of 25%. Retirement plan distributions associated with pre-tax contributions will be taxed upon withdrawal. Information and interactive calculators are made available to you as self-help tools for your independent use and are not intended to provide investment advice. We cannot and do not guarantee their applicability or accuracy in regard to your individual circumstances. All examples are hypothetical and are for illustrative purposes. We encourage you to seek personalized advice from qualified professionals regarding all personal finance issues. We do not provide investment OR tax advice. Please consult a tax advisor for more information.

Speaker Text:

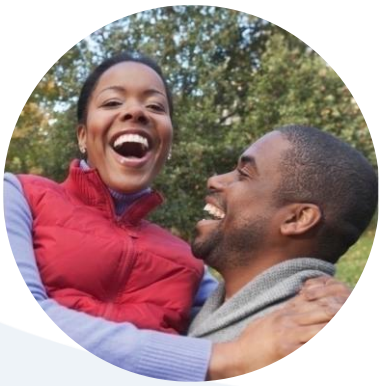
Let's look at Rita's situation. As a working mom, Rita's juggling a lot of financial priorities. She feels like she can't afford to have any more money come out of her paycheck.

However, when you look at it closely, you can see how little an impact it will make in Rita's weekly take-home pay, while giving her tax savings and potentially making a significant difference in how much she could have at retirement.

Know your Roth

A *different* type of contribution within your retirement plan

- After-tax contributions; future tax-free income*
- Both traditional pre-tax and Roth elective deferral contributions are possible
- Employer contributions are made to your account on a pre-tax basis only

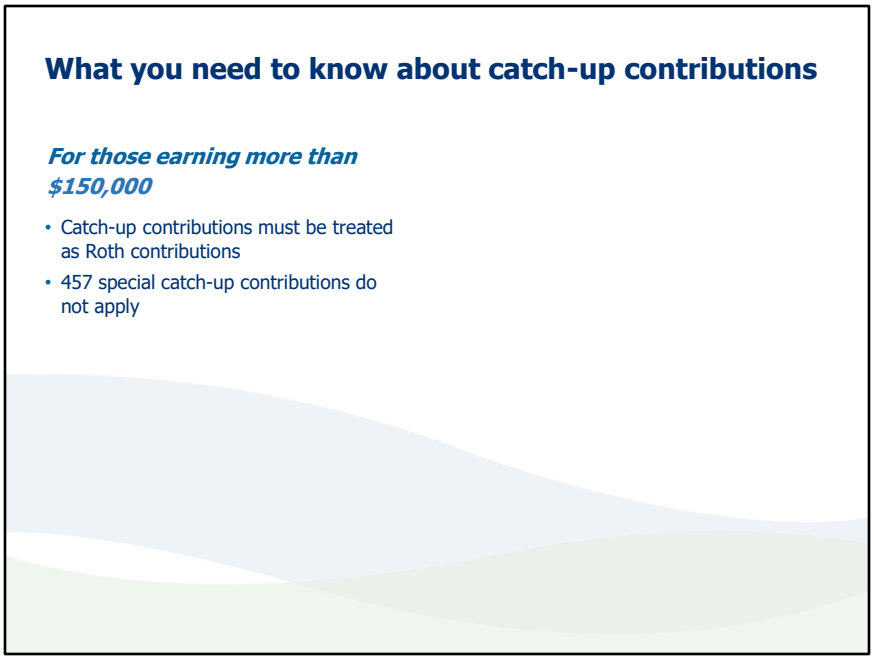


* Generally, for distributions of Roth contributions to become qualified for federal income tax purposes, you have to wait at least 5 tax years after making your first Roth contribution before taking a withdrawal, and your withdrawals must begin after: you have reached age 59½; your death; or you have become disabled. If your withdrawal does not meet these qualifications, your accumulated Roth earnings—but not your Roth contributions—will be taxed, and may be subject to a 10% early distribution penalty if you have not reached age 59½. State tax treatment may vary. Roth 457 non-qualified withdrawals are not subject to a 10% early distribution penalty.

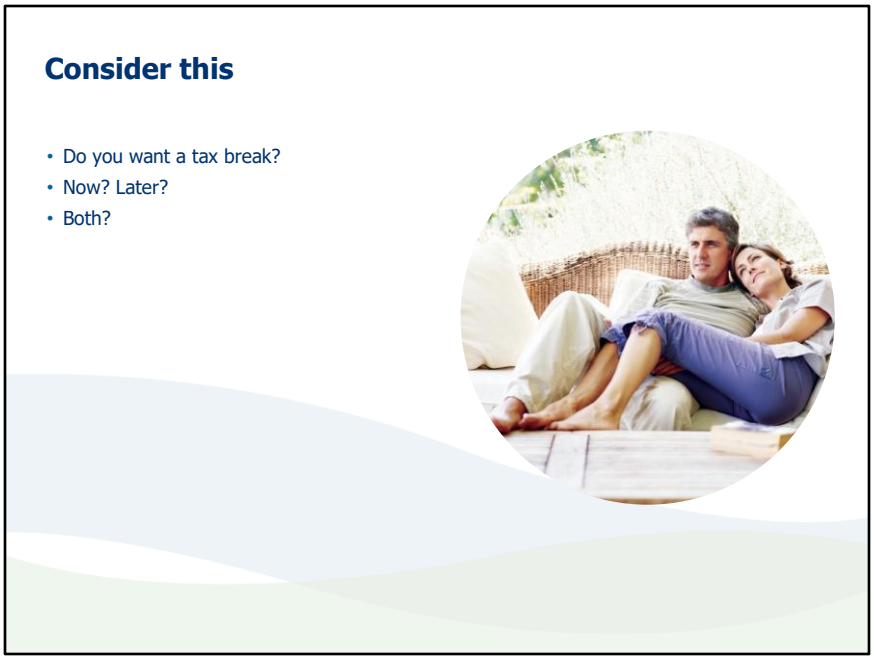
Speaker Text:

But all your contributions **don't** have to be made on a pre-tax basis.

[read slide]


What you need to know about catch-up contributions
For those earning more than $150,000
• Catch-up contributions must be treated as Roth contributions
• 457 special catch-up contributions do not apply

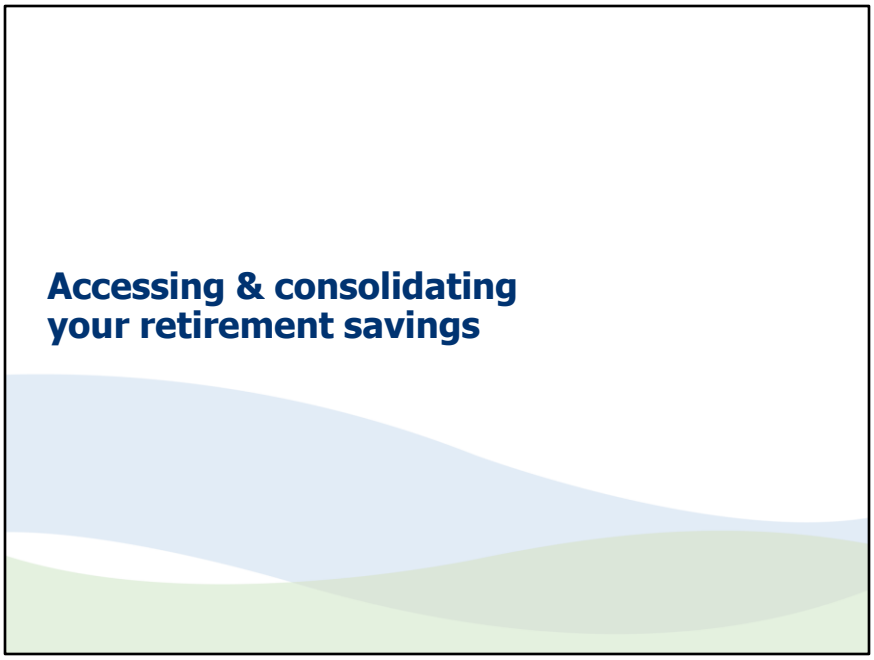
[read slide]



Speaker Text:

When choosing between pre-tax contributions and Roth contributions, here are some important questions to ask yourself. Keep in mind, you can make *both* types of contributions.

[read slide]



[Read slide]

Access to funds while working

- Loans
- In-service distributions
- Hardship withdrawals



[Read slide]

What happens when you leave your job?

- **Do nothing!** Keep your funds in the Plan
- **Roll over to an IRA** or a new employer's program
  - If you remain an NC public employee, you may continue contributing through your next employer
- **Begin withdrawals***
  - Installment payments
  - Partial withdrawal (on an as-needed basis)
  - Lump-sum withdrawal
- **"Transfer Benefit"** – move pre-tax assets to TSERS/LGERS to generate monthly income
  - Guaranteed lifetime payout
  - May elect survivor options and refund feature
  - **www.NCLifetimeIncome.org**

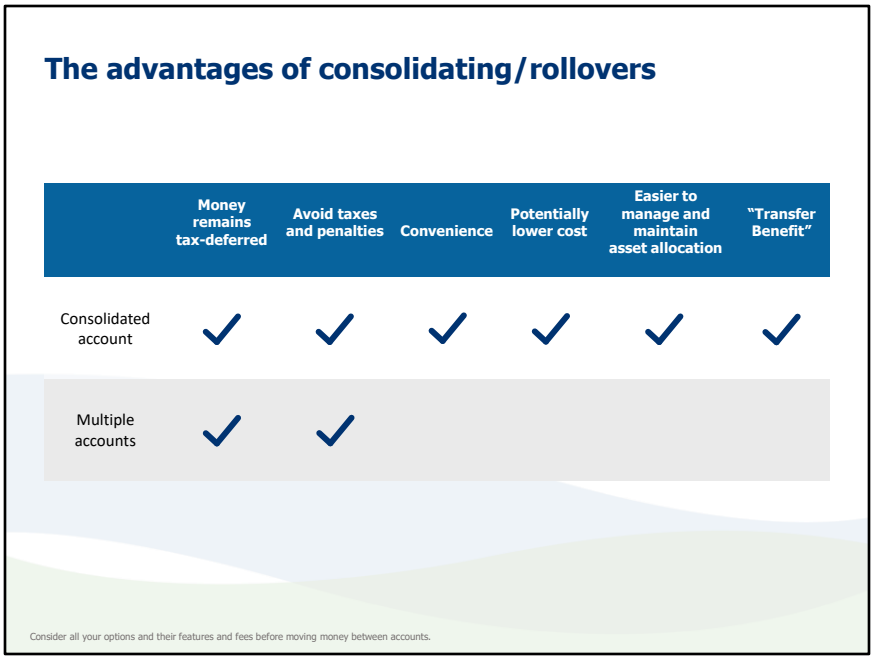


* Payments are subject to a mandatory 20% federal income tax withholding, and for withdrawals from the NC 401(k) Plan, may be subject to a 10% tax penalty if taken prior to age 59½. Please note that if you terminate from service, requests for withdrawals or distributions from your account (not associated with retirement) will not be paid for 60 days, unless you are: (1) retired; (2) eligible for an in-service distribution; or (3) required to take a distribution by the Internal Revenue Code or the provisions of the Plan.

It's important to know, too, that you have a number of options for withdrawing your funds.

- You can keep your funds in the Plan.
  - You can leave your assets in the Plan until age 73, when you must begin making minimum withdrawals. (Provision 107)
  - Due to Secure 2.0 legislation, however, the required minimum distribution (RMD) requirement does not apply to any assets designated as Roth within your Plan account. (Provision 325)
  - In addition, a surviving spouse may elect to be treated as the deceased plan participant for purposes of the RMD rules. (Provision 327)
- You can roll these assets into an Individual Retirement Account
- If you go to a new employer, you can roll these assets into the new plan, if your new employer accepts rollovers
- You elect a systematic payment option; for example, you may choose to have your assets disbursed monthly, quarterly, semiannually or in annual installments
- You can have the money sent to you in a lump sum or simply take it out on an as-needed basis
- You can utilize the Transfer Benefit by moving pre-tax assets to TSERS/LGERS to

generate monthly income



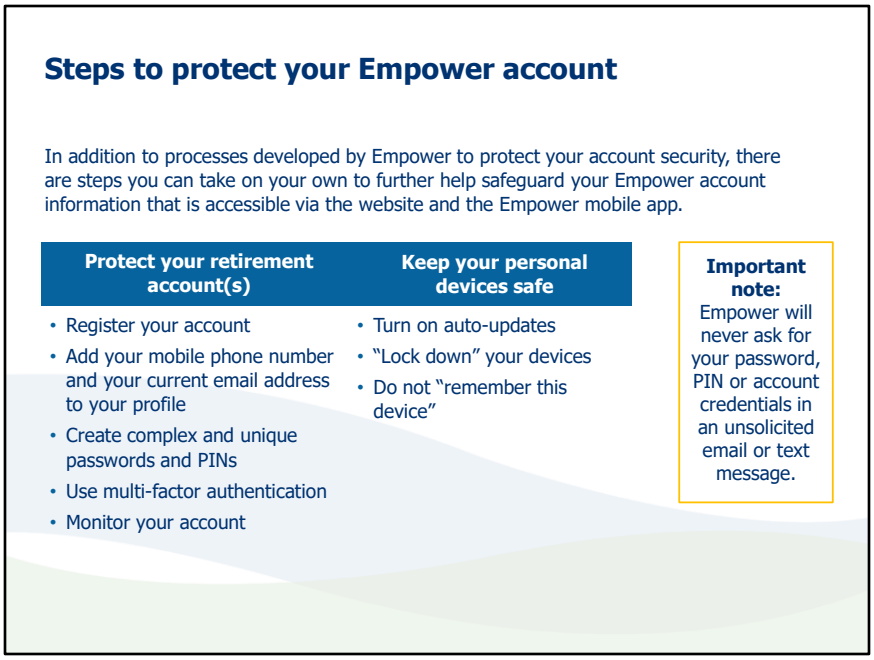
Speaker Text:

This might be a good time for you to consider moving money from *other* employer-sponsored plan accounts you may have to the NC 401(k) Plan or NC 457 Plan.

[Read slide]



Now let’s review how you can protect your online NC 401(k) and/or NC 457 account.



Register your account

Log in and register your Empower account to reduce the chance that someone else can access your account or take your account over. Check your account frequently and pay close attention to security alerts.

Add your mobile number and your current email addresses to your profile

The best way to protect your accounts is to use the recommended security protections described on this website and provide current contact information — including your mobile phone number, email addresses and mailing address.

If our only communication option is through an email address that has been hacked or compromised, then we're only communicating with the fraudster. Create complex and unique passwords and PINs.

Change your passwords often and don't reuse passwords. You can reset your password only through our secure website.

Password reuse provides the easiest way for a criminal to access your accounts. Use multi-factor authentication.

Your Empower account has multi-factor authentication, which sends a one-time code to your phone or email allowing you to access your account securely. Multi-factor authentication requires access to another device, which improves the security of your account. Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.

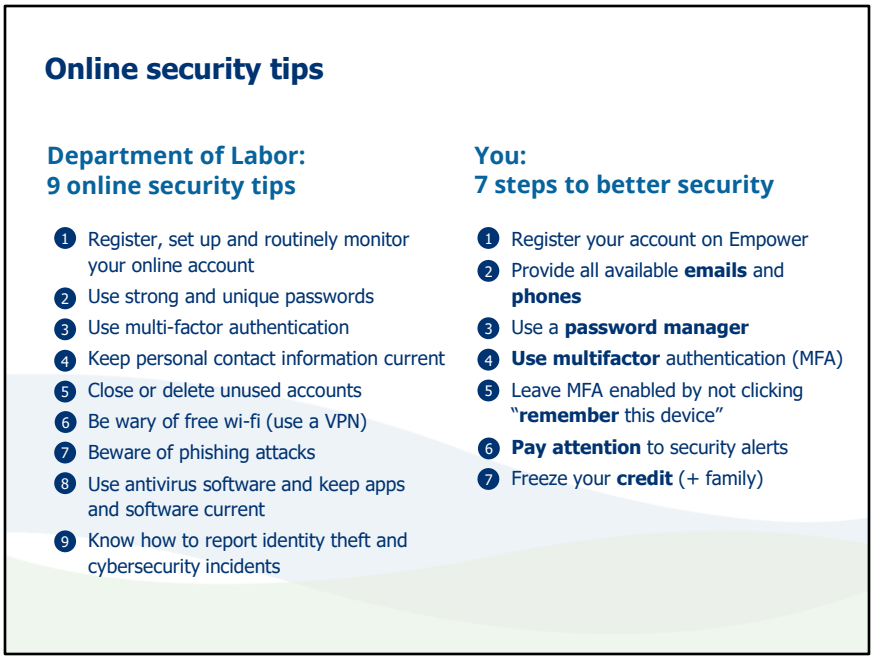
It's harder to hack a mobile phone than an email account; consider using text message for multi-factor authentication rather than email.

Monitor your account

Receive status notifications that inform you of account activity by enabling them in your account preferences. Review security alerts immediately. If you see account activity you didn't request, contact Empower right away.

Empower will never ask for your password, PIN or account credentials in an unsolicited email or text message.

Turn on auto-updates
Always keep your browser, applications and operating system updated. Maintain up-to-date anti-virus, anti-malware and firewall software on your devices.
"Lock down" your devices
Password protect your mobile, wearable and computer devices.
When not using your devices, use the built-in security functions such as the keypad lock.
Wipe your phone of all personal data before discarding or selling it.
If you lose your phone or change your number, sign in to your Empower account to remove the old number from your profile.
Do not "remember this device"
It's best to always use multi-factor authentication (MFA) and to not remember your devices. The additional 10-15 seconds it takes to use MFA makes it much harder for a criminal to log in to your accounts. Choosing to remember a certain device will deactivate multi-factor authentication for future visits, which provides a faster login experience but is riskier.



The Department of Labor's "Online Security Tips" provides guidance for Plan participants and beneficiaries to reduce the risk of fraud and loss in their retirement accounts. Each of the (9) nine DOL Online Security Tips are comprehensively addressed by Empower on the Empower's "Security Tips" website.

You can reduce the risk of fraud and loss to your retirement account by following these basic rules. Empower's version is specific to our accounts and ours are in order of priority.

If we can get participants to do 1 thing, it's register their account. Simply put, Create a username, password and beneficiary information.

1. It is **Easier** for a fraudster to pretend to be you if you don't register your account.

We have a large number of accounts that employees never claim / register. Maybe the reason includes that there's not a big balance, or they are so far away from retirement, or they feel it would be safer not to log on, but in fact it couldn't be further from the truth. Your account is already online and if you don't claim it, it does make it easier for a criminal to register the account. To pretend to be you and take money out on your behalf.

Register, set up and routinely monitor your online account

Use strong and unique passwords. Use multi-factor authentication. Keep personal contact information current. Close or delete unused accounts. Be wary of free wi-fi (use a VPN). Beware of phishing attacks Use antivirus software and keep apps and software current. Know how to report identity theft and cybersecurity incidents.

2. If I can get you to do two things, the second is to give us all your available emails and phone numbers. Not so we can spam you, not so we can sell those – because we don't do that. (Retirement is our only business and we don't have a reason to cross-sell like others.) It's just for security alerts. If we see unusual activity on your account, we send security alerts to all the emails and all of the phone numbers that you provided. The #1 crime that the FBI is investigating today is Business Email Compromise **(BEC & Email Account Compromise).** And that is simply someone has taken over your work or personal email account. And if that's the only point of contact we have for you, that email account, it means that if a fraudster has taken over that email account, that means I'm only going to talk with that fraudster. Every notification, every alert, every confirmation I send to you is only going to go to the bad actor, who will delete all security alerts before you see them. (You may have no opportunity to tell your bank or recordkeeper that wasn't you and please stop before the money goes out the door.)

3. Use a "commercial" password Manager. (Can password managers be breached? The quick answer is "yes." But password managers have strong encryption. And while cybercriminals may get "in," it doesn't mean they will get your master password or other information. The information in your password manager is encrypted. And deciphering that encryption, which is usually industry-standard encryption like Advanced Encryption Standard (AES), is almost impossible. Plus, most password managers do not store or have any access to your master password or the encrypted information in your password database. If the password manager itself is breached, the data in your password manager is encrypted and stored elsewhere, and password managers **do not retain your master password.** Much of the security of your password manager depends on the strength and safety of your one master password. And for many password management systems, that master password is not stored on the same server as your encrypted information. This adds an additional layer of security.)

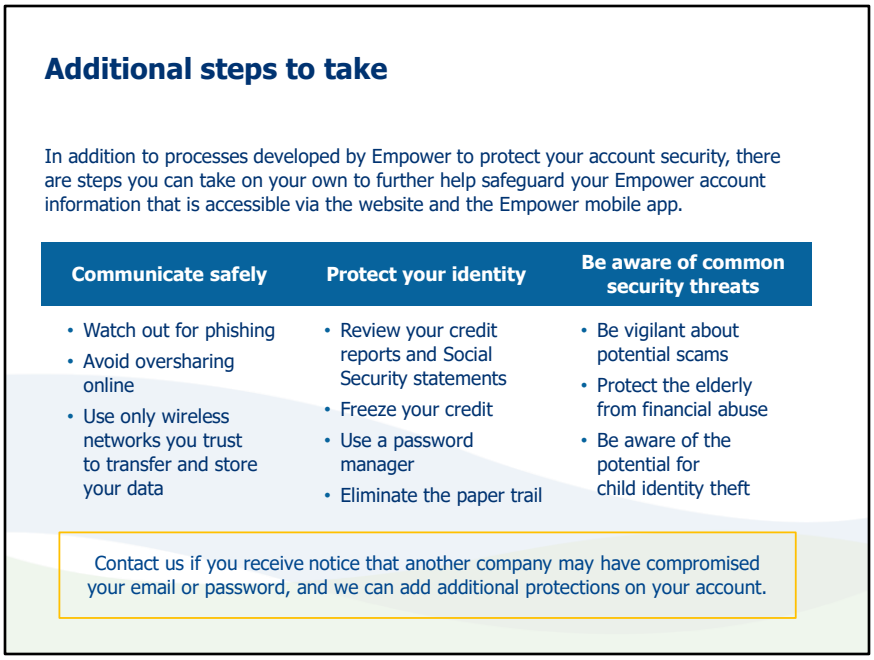
4. **Do not have browsers, like Safari, Chrome or Microsoft Edge remember your username, password or device.** Browsers may not be updated regularly, nor do you need to MFA into your browser like a commercial password manager.

5. Multi-factor authentication – The #1 way I can prevent criminals from easily accessing my account is by using MFA for every account. Without MFA, fraudsters just need to have knowledge. Knowledge of my username and password. MFA adds possession. They need to possess another device - your cell phone or SIM card or email address. **Use MFA for every account, including email, and never disable it.** Text is preferred to email for MFA since it's harder to hijack a phone's SIM card than an email account.

6. **Leave MFA enabled by not clicking "remember this device."** This will enable MFA, which minimizes the chance that a cybercriminal can break into your account.

7. **Always pay attention to security alerts.**

8. **Freeze your credit,** for you, your family, nieces and nephews. Freezing your credit is a best practice and it is free with the 3 major credit card bureaus. The only time you need to unfreeze your credit is when you need new credit to buy a car, refinance a home or something like that. Freezing your credit vastly reduces the chance that a bad actor can take out credit on your behalf even if they have your identity.



Watch out for phishing
Don't open suspicious attachments and take precautions when downloading applications. Don't provide your Social Security number, birthdate, account numbers, passwords or PINs to anyone unless you have initiated the contact.
Use secure websites and always log out when finished. Look for a lock symbol in the address bar (or in your browser window) and a web address that begins with https://. Make sure the https:// is on every page — not just the login page. Unless you have initiated the contact, never log in to your account or re-enter your password via a link sent from a text message — go to the original source.
Avoid oversharing online. Don't share any information that is used by your financial institutions to verify your identity. Review the privacy settings for your social media accounts and never share your username, passwords or PIN with anyone. Do not share your device authentication such as Face ID or Touch ID with others.
Use only wireless networks you trust to transfer and store data. Always change your home router's password from the factory default password. Protect your wireless networks and routers with complex passwords. Never use free or public Wi-Fi to access your financial accounts. Don't store personal information on websites unless they use good security features, such as a required sign-on, data encryption and https://. Be cautious using online storage and make sure the settings are not set to "public view." Avoid using public computers for financial activity. If you do, clear the browser's history and cookies before you log off.

Review your credit reports and Social Security statements. Check your credit reports at least annually to ensure no one else is using your identity. Identity thieves will try to use your Social Security number, birthdate, driver's license, passwords and account numbers (including rewards accounts), to open new

credit cards or loan accounts, divert communications, change your passwords, and commit fraud for financial gain.

Freeze your credit. This combats identity theft and credit fraud by making it impossible for anyone to take out credit on your behalf — even if they have your full identity. You can unfreeze your credit with the three major credit bureaus when needed.

Use a password manager.

Eliminate the paper trail. Save downloads locally on your computer or on an encrypted storage device. If you do print documents with financial information, be sure to shred them before discarding.

Be vigilant about potential scams. Strangers may try to trick you into giving up your personal, bank or credit card information as well as money or property. These situations may include, but are not limited to:

- Scammers posing as computer anti-virus support
- Shop-at-home and catalog sales
- Prize giveaways
- Technical support employees
- IRS/Medicare/Social Security Administration representatives
- Grandchildren reportedly in trouble
- Love interests (romance scam)
- Reloadable gift card requests
- Lottery/sweepstakes officials

Scammers may also offer you money with the intent of gaining access to your financial bank account information.

Contact us if you receive notice that another company may have compromised your email or password, and we can add additional protections on your account.

Protect the elderly from financial abuse. They may have significant assets or home equity and usually have a regular source of income, like Social Security, a pension or annuities. Raise awareness of the dangers of financial abuse with loved ones who may be susceptible to fraud. It's recommended that the elderly communicate frequently with friends and family, as isolation is often a contributing factor to abuse. Watch out for signs of financial abuse by caregivers or relatives, including requests for unexpected payments.

Be aware of the potential for child-identity theft. Children are often a target of identity theft, and it is often perpetrated by a family member who may have legitimate access to the child's personal information. Warning signs of child-identity theft include a child receiving:

- Pre-approved credit card offers
- A credit card bill
- A jury summons
- Driver's license renewals
- Bills for medical care or other purchases
- Collection notices



If you suspect any unusual activity on your Empower account, let us know immediately. **Contact Empower at 866-627-5267 so we can add additional protections to your account.**

Change your password and, if you have reused the compromised password, change it in all places. Change all email passwords and add multi-factor authentication to your email accounts.

Then notify all of your financial institutions.
Notify all three credit bureaus:

- Equifax: **888-202-4025** or equifax.com
- Experian: **888-397-3742** or experian.com
- TransUnion: **800-680-7289** or transunion.com

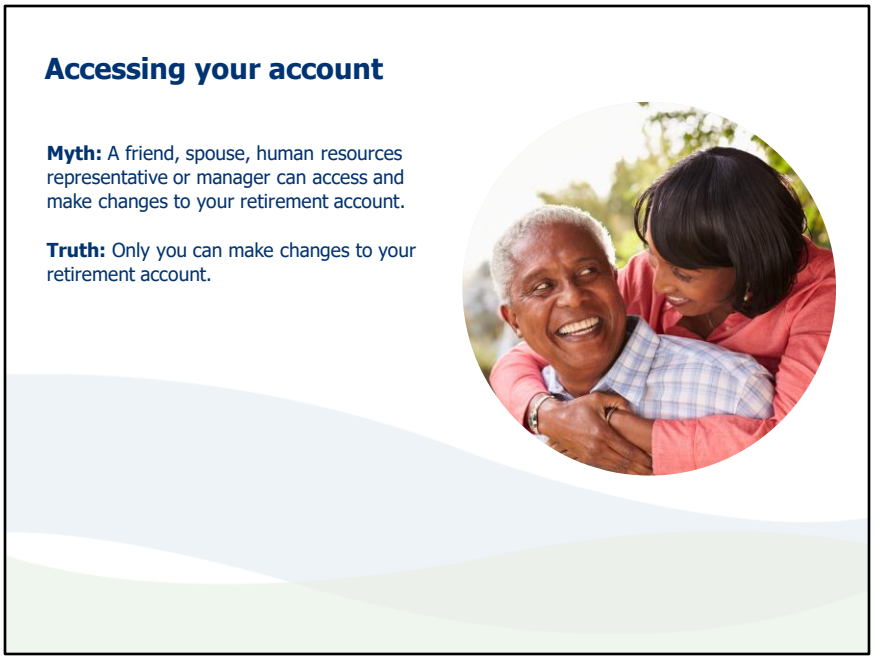
If you are a victim of online crime, file a report with the FBI's Internet Crime Complaint Center (IC3.gov) as soon as possible.

Empower Retirement, LLC and its affiliates are not affiliated with the author or responsible for third-party content provided.

The credit bureaus listed are not affiliated with Empower Retirement, LLC and its affiliates.

These best practices are for informational purposes only. They apply to U.S. residents. Security risks and recommendations change frequently. Check this site for updates. Follow the alerts,

recommendations and announcements from your service providers, law enforcement agencies and consumer protection agencies.



Myth: A friend, spouse, human resources representative or manager can access and make changes to your retirement account.

Truth: Only you can make changes to your retirement account.

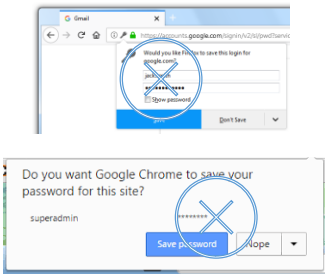
What people often don't realize is that others need permission to discuss your account. In fact, changes can't be made to your account by anyone else but you, unless there is a power of attorney on file. Spouses, friends, human resources reps and managers can't make changes to your account. Be sure to keep passwords safe in order to safeguard your account.

Password managers

Myth: All password managers are considered equal.

Truth: It is not recommended to use browsers (like Chrome, Firefox, Safari) to store your passwords. You don't need to multi-factor authenticate into your browser. Browsers can be out of date without the latest patches, and it is not a good user experience across your various devices, if you're using different browsers.

Pro tip: Commercial password managers (like Lastpass, 1Password and KeePass) are more secure and range from free to up to $30 per year.



FOR ILLUSTRATIVE PURPOSES ONLY.

LastPass 1Password KeePass

The password managers listed are not affiliated with Empower Retirement, LLC and its affiliates.

Password Managers

Myth: All password managers are considered equal.

Truth: It is not recommended to use browsers (like Chrome, Firefox, Safari) to store your passwords. You don't need to multi-factor authenticate into your browser. Browsers can be out of date without the latest patches, and it is not a good user experience across your various devices.

Pro Tip: Commercial password managers (like Lastpass, 1Password and KeePass) are more secure and range from free to up to $30 per year.



Empower is committed to maintaining the highest level of online security and the protection of personal information and accounts.

All of our **security**, all our **processes**, and all our **auditing** that we have in place is backed by our **Security Guarantee**.

To summarize it, if through no fault of your own, you have money taken out your account, we will make you whole. It's a simple as that.

We take on this responsibility in part because we believe so strongly in the security practices and validation that we've put in place, **and our** ability to identify that fraud or criminal activity is happening **inside** of your account.

We realize the inherent trust we place in our financial institutions and thank you for your continued trust.

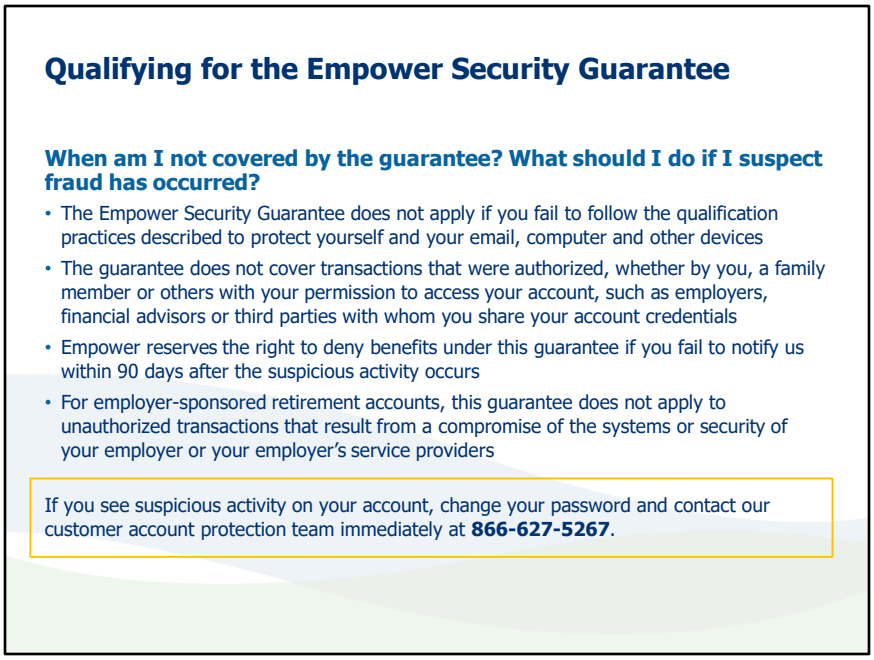


How do I qualify for this protection?

Your Empower accounts are automatically eligible for this protection when you follow the online and mobile security practices below and more fully described in our Security Tips located in the Security Center at Empower.com.

Online and mobile account security is a shared responsibility. Let's work together to protect your account.

1. Register your account, then keep your contact information current.
2. Protect your personal and financial information.
3. Review your accounts.
4. Increase login protection and keep device updates current.
5. Look out for suspicious emails, texts and phone calls.
6. Check this page periodically for updated information, as we proactively monitor evolving cybersecurity threats.



Qualifying for the Empower Security Guarantee

When am I not covered by the guarantee? What should I do if I suspect fraud has occurred?

- The Empower Security Guarantee does not apply if you fail to follow the qualification practices described to protect yourself and your email, computer and other devices.
- The guarantee does not cover transactions that were authorized, whether by you, a family member or others with your permission to access your account, such as employers, financial advisors or third parties with whom you share your account credentials.
- Empower reserves the right to deny benefits under this guarantee if you fail to notify us within 90 days after the suspicious activity occurs.
- For employer-sponsored retirement accounts, this guarantee does not apply to unauthorized transactions that result from a compromise of the systems or security of your employer or your employer's service providers.

If you see suspicious activity on your account, change your password and contact our customer account protection team immediately at **866-627-5267**. Report any suspected incidents, activity, unreceived account statements or unauthorized activity to us immediately and cooperate with us as we look into the matter.



[read slide]



Speaker Text:

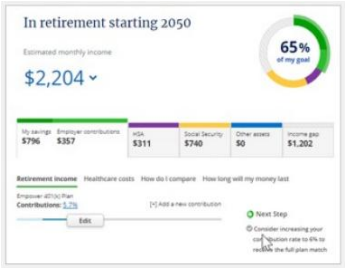
Your Plan offers you some terrific, easy-to-use tools that are designed to help you:

- Each quarter, Empower will provide an easy-to-read retirement statement that includes all the information about your account, including fund performance, your account value, tips on how you can save more, important updates from your employer, and more. You may elect to access your statement online, for added convenience and security, rather than receive it in the mail.
- Empower also offers quarterly newsletters to all Plan participants. If you receive your quarterly statement in the mail, your newsletter will be included. Otherwise, you may access the newsletter online.
- Your annual MARS Statement provides a snapshot of your current and future potential pension benefit.
- You can also take advantage of our toll-free phone service by calling **866 NC PLANS,** where you can obtain account information or perform transactions through your telephone keypad.
- Empower's participant website, **myNCPlans.gov**, with its easy-to-navigate tabs, makes it a breeze to find the information you need and to process your transactions online. Simply visit **myNCPlans.gov** to quickly view your account details, transfer money between investment options, increase your contribution amounts, change investment options, check fund performance, and review, print, or request online statements. It's also a great place to visit when retirement is just around the corner.

Now let's take a closer look at the last two tools—the Retirement Income Estimator Tool and your NC 401(k)/NC 457 Plans' Retirement Plan Counselor.

Retirement Income Estimator Tool

- Know where you stand
- See where you're going
- Save your way
- Retire your way



FOR ILLUSTRATIVE PURPOSES ONLY.

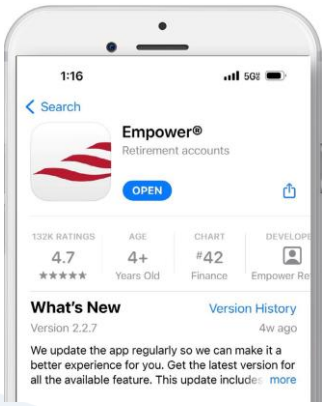
Speaker Text:

The Retirement Income Estimator Tool can help you check your progress along your retirement planning journey. It is located on your personal dashboard and is updated every time you log in to your account.

This valuable tool helps you track your retirement savings percentage to goal — and model any potential changes to your savings. It is a great tool that is designed to help you ensure you are on track for the kind of retirement you have always imagined.

The Empower mobile app

- Log in anytime, anywhere
- Access the app in your preferred language
- Monitor your savings and performance
- Change your contributions and investments



FOR ILLUSTRATIVE PURPOSES ONLY.

Download on the App Store

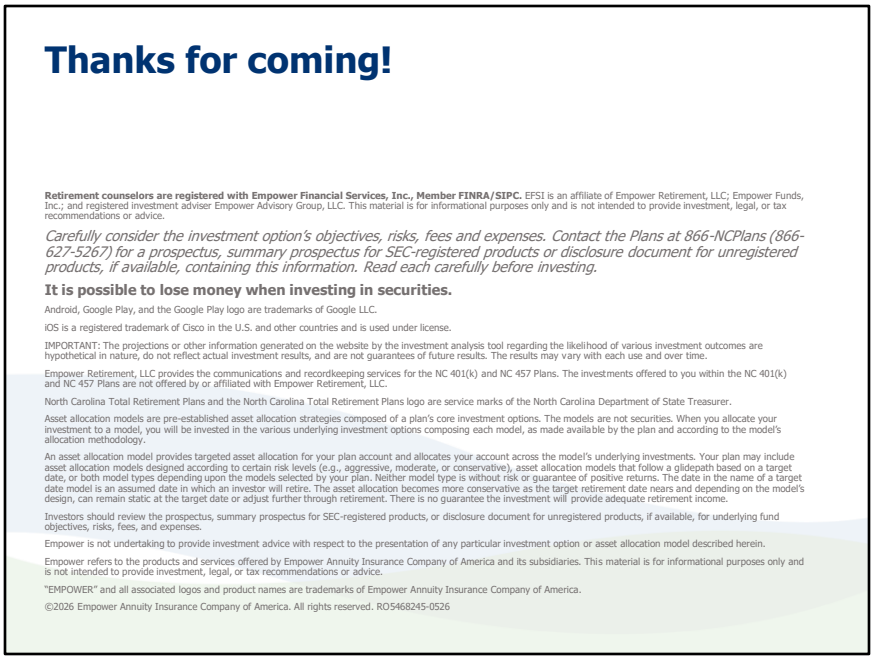
GET IT ON Google Play

[read slide]



Finally, your dedicated NC 401(k)/NC 457 Plans' Retirement Plan Counselor can provide you with personalized support to help you make sense of it all. Best of all, you can set up a virtual meeting with your counselor.

So as you can see, when it comes to the Supplemental Retirement Plans, we put the help you need at your fingertips!



Speaker Text:

Thanks so much for coming to our presentation today. I encourage you to take what you've learned here, along with the tools that Empower provides and get started on your retirement. But be sure to act today to protect your tomorrow.