



Quick Tips: Defend Against Fraud

What is phishing?

Phishing is a social engineering scam that tricks users into disclosing sensitive personal information or clicking on malicious links.

The FTC¹ outlines some common stories phishing scammers use:

- Saying they've noticed some suspicious activity or log-in attempts — *they haven't*
- Claiming there's a problem with your account or your payment information — *there isn't*
- Saying you need to confirm some personal or financial information — *you don't*

Tips to prevent phishing

- Never provide personal information in response to an unsolicited request
- If you receive an alarming email, contact the company who sent it using the official company email address or phone number
- **Do not click on links** if the email or text message seems suspicious
- If you mistakenly provide sensitive information, contact one of the three major credit bureaus to place a fraud alert on your file. This prevents thieves from opening accounts in your name
- Report the phishing attempt to the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/identity-theft/identity-theft-report).

Tips to prevent unauthorized access

- Never give your personal login credentials to anyone else
- Lock written passwords, checkbooks, and account statements out of sight
- If you save passwords on your computer, make sure your computer is locked with a password
- Only allow Power of Attorney to be signed over to someone you trust
- Do not let hired caregivers or helpers open your mail, pay your bills, or manage your finances.
- Review your accounts regularly for inconsistencies and purchases you do not recognize

If your information has been compromised

- Change your passwords immediately
- Alert your bank(s) that someone may have access to your account(s)
- Report identity theft to the Federal Trade Commission (FTC) and get a recovery plan
- Contact your Diversified Advisor

¹ <https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams#recognize>



Diversified

EXPERIENCE LIFELONG WEALTH

IDENTIFYING LEGITIMATE DIVERSIFIED CONTACTS

Your advisor will reach out to you if action is needed on your accounts, and for regular account check-ups. If we need to contact you:

- All emails from Diversified will come from the official *diversifiedllc.com* domain
- We will **never** ask you for sensitive Personally Identifiable Information (PII) via text message or unencrypted email.
- Any Associated Person who contacts you will first identify themselves by name
- If we have concerns about your account's security, your advisor will call you or your designated emergency contact to discuss the situation in a calm, non-threatening manner

If you experience any of the following, report it to your advisor immediately. Do *not* click any links or provide any information to suspicious contacts:

- An email, text message, or phone call from anyone other than your advisor or advisor's planning team requesting sensitive PII
- An email claiming to be an employee of Diversified, LLC that comes from an email address other than *diversifiedllc.com*
- Threatening phone calls or alarming messages intended to make you fear your accounts or data have been compromised by using language such as *urgent action required*, or *act now to avoid reporting*

RESOURCES

[Report Identity Theft](#) – This website from the Federal Trade Commission (FTC) is dedicated to helping victims report identity theft and create a recovery plan.

[Report cyber crime](#) - The Internet Crime Complaint Center (IC3) is part of Federal Bureau of Investigation and you can report several different types of cyber crime here

[How to Avoid Phishing Scams](#) – An article from the Federal Trade Commission (FTC) with excellent tips on preventing phishing, and examples of what phishing emails may look like.

[Money Smart for Older Adults](#) – a guide for adults of all ages containing tips about staying safe and financially secure. Includes information on common scams and elder abuse.

[Elder Justice](#) - This is an initiative through the Department of Justice whose mission is to combat elder abuse, neglect, and financial fraud and scams that target older adults.