BPAS

Cybersecurity Policy

An Addendum to the Policy Statement Regarding Account Transactions at BPAS

In today's information age, data on American consumers is everywhere. Protecting the security of your retirement accounts is a top priority at BPAS; however, we can't do it alone. Protecting participant accounts is a shared responsibility between participants, service providers and employers. This cybersecurity policy outlines steps you need to take as a participant to enhance your chances of recovery if fraudulent activity or identify theft occurs within your account and provides assurances from BPAS on this important matter. Please note that BPAS will evaluate each situation based on the specific facts surrounding any fraudulent activity.

As a routine part of our security procedures, BPAS conducts periodic audits of our Information Technology infrastructure. We use firewalls, antivirus software, security fixes, and other measures to protect our systems. Our websites rely on industry-standard encryption to protect data transmission and access, while our IT staff closely monitors security alerts and applies updates as needed.

We recommend you use a browser that supports encryption, is JavaScript enabled, and accepts cookies. These measures allow us to track usage of the site and improve our service to you.

It is best for you to use the latest version of one of these browsers to access your BPAS account: Microsoft Edge, Firefox, Google Chrome, or Safari.

BPAS will continue to identify new tools and implement features in our online systems to help ensure that your data and assets are protected.

Although these tools and features help, you are the most critical element in protecting your account.

Fraud Prevention Tips

- If an offer is made that seems too good to be true, it probably is.
- Sharing your login credentials with any outside party or software application (for any reason) will invalidate the ability to collect damages if there is fraud involving your account.
- An attacker will try to trigger your emotions, for example urgency or fear, in an attempt to get you to act quickly.
- Limit the information you put in your social media profiles. An attacker can use these sites to collect valuable information and use it to commit fraud on you or family/friends. Also, be wary of games or tests in your social media. Many of these tests are created by fraudsters looking to gather personal information about you, like names of family members, important dates, favorite colors, etc. This information makes it easier for them to impersonate you and answer security questions.
- Question unsolicited emails containing attachments, especially if they require you to enable macros, as they are potentially malicious.
- Keep in mind that an email account of a friend or family member could become compromised. Attackers can spoof a sender's email address to appear to be from anyone they choose. If you receive a suspicious email, reach out to confirm whether they intended to send it.
- Some of the most common places where social engineering attacks take place are via email, text message, or even by phone.
- Tech-support scams often begin with phone calls from an attacker who claims they are from a well-known company. They will try to convince you that your computer is infected with viruses. You should hang up the phone immediately.
- When logging into your BPAS account, or transmitting any confidential information, type the address into the URL. Don't click on links from an email or search engine. Also be certain the address in the URL shows it is a secure site (https, not http).
- Use secure protocols and the BPAS secure messaging center when transmitting confidential information; email should be a last resort, because it can become compromised.
- Keep your internet browsers updated. Make sure the physical mailbox at your home is safe, or use a PO Box.
- Install anti-virus and malware protection on your home computer and enable auto updates.
- Don't open emails or attachments from senders you don't know or that appear suspicious.

BPAS

Recommended & Required Security Steps

Below is a list of the **recommended** and **required** steps you must take to protect your account to maximize your chances of recovery in the event of external fraud. If fraud is suspected to have occurred within a participant's account, the situation will be researched by BPAS with appropriate financial institutions and law enforcement to determine follow up steps and the responsibility of all parties. The speed of this process to resolve any disputes will be driven by outside institutions and law enforcement. Your ability to seek recoveries will be dependent upon the actions you take to protect your account as reflected below.

Action	Recommended	Required
Create a User ID that is unique to you and not easy to guess. Don't use your Social Security Number or email address as your User ID.	✔	✔
Use a strong password in your account: • Follow required parameters that combine letters, numbers and symbols • Avoid predictable keyboard patterns • Don't use the same password for multiple sites and accounts • Don't use your User ID as your password • Never share password • Change password every 90 days, or immediately if any concerns	✔	✔
Do not store your User ID and Password on your phone except in a secure password-keeping app, and don't select "Remember Password" in your browser.	✔	
Login and review your BPAS account at least monthly.	✔	
Update your account at u.bpas.com to include a current, personal email address that you regularly monitor and access, **which will be visible on your mobile phone immediately when you receive an email**. BPAS will send you email alerts when account changes are initiated or attempted.	✔	✔
Monitor emails you receive from BPAS, review account activity and notify us immediately (within 1 business day) of any questionable activity.	✔	✔
Open and review mailed confirmations immediately upon receipt.	✔	✔
Don't login to your BPAS account from a public computer or use public WIFI.	✔	
Comply in good faith if we ask for your cooperation in an investigation (including having a professional computer security company review your computer, police investigation, etc.).	✔	✔
Monitor your mailbox and promptly review all statements and correspondence from BPAS.	✔	✔
Make sure your mailing address is up to date at BPAS at all times.	✔	
Do not use an account aggregation service that requires you to submit your User ID or password to an outside firm.	✔	✔
Do not click on links or open attachments in emails from senders unfamiliar to you.	✔	
Maintain up-to-date spyware on your laptop/computer.	✔	
BPAS will never ask you to provide personal or account information via email. Notify BPAS within 24 hours if you suspect or note suspicious account or email activity.	✔	

Questions? Let's Talk.

Protecting the security of your accounts is a shared undertaking, and we're here to help.
Please reach out with any questions or concerns.

u.bpas.com **1.866.401.5272**