Don’t Get Scammed

We’ve noticed an alarming increase in scamming attempts. Here’s a list of the latest:

1. **Scam: PSE&G calls threatening to disconnect your service if you don’t immediately pay several hundred dollars in past due bills**. The caller will insist that you pay using some kind of gift card. **Or you are offered a 20% rebate** for being a wonderful customer. **The Reality**: Neither PSE&G nor Jersey Central makes these calls or offers rebates for being a good customer. **Remedy**: Hang up.
2. **Scam: While viewing a website, a pop-up appears warning you that your computer has become infected** and to call Microsoft at the phone number listed. **The Reality**: Microsoft doesn’t monitor your computer. **Remedy**: Close your browser. If you can’t, hold the power button for fifteen seconds to force your computer to shut down and then restart it.
3. **Scam: You receve an email confirming an online purchase you never made**. The message includes a phone number to call to arrange a refund. **The Reality**: The scammer will trick you into sharing your online banking website. **Remedy**: Ignore the email. You can always log in to your online retailer to confirm purchases and request refunds.
4. **Scam: You receive an email that you’ve been observed visiting an adult website**, and that if you don’t pay $5,000 in Bitcoin, the scammer will tell all your acquaintances and include pictures of you visiting the site. The email may include one of your passwords as “proof .” **The Reality**: It’s difficult, if not impossible, for someone to monitor your site visits. **Remedy**: Ignore the threat. However, if you use that password for any of your accounts, you should change it.

## To protect yourself

1. Don’t respond to emails or phone calls demanding money, especially if they demand payment in crypto-currency (e.g. Bitcoin) or gift cards.
2. Don’t respond to pop-up banners claiming that your computer is infected.
3. Don’t call phone numbers listed in threatening emails.
4. Don’t allow anyone you don’t know to remotely control your computer.
5. Request help from our [Tech Resources](https://princetonsenior.wufoo.com/forms/technology-assistance-request/) if you suspect a scam.