



Secure and Protect | Phishing

As your enduring financial partner AB&T is always looking out for you, especially when it comes to protecting your personal and financial information.

One of the most common threats today is phishing, where scammers try to steal your sensitive information by pretending to be a trusted organization.

What You Need to Know About Phishing

Phishing typically involves emails, texts, or calls that look like they're from a legitimate source, such as your bank or a government agency. In reality, they're from cybercriminals trying to get you to share personal information like passwords or account numbers.

And they are only getting more aggressive. The Federal Trade Commission reported that phishing scams accounted for nearly 36% of all reported fraud cases, and cost consumers over \$2.3 billion in 2023 alone, illustrating just how widespread and damaging these attacks can be.

But we're here to help.

How to Spot a Phishing Attempt

Here are a few signs to watch for that might indicate a phishing attempt:

- **Urgent or Scary Messages:** Phishers often use urgent language, claiming there's a problem with your account or that you've won a prize to make you act fast.
- **Strange Email Addresses or Numbers:** If something looks off about the sender's contact details, be cautious.
- **Suspicious Links or Attachments:** Never click on links or download attachments from unknown sources. Instead, hover over links to see where they really lead.
- **Requests for Personal Information:** Legitimate companies will never ask for sensitive information like passwords or Social Security numbers via email or text.

How to Protect Yourself

Here are a few ways you can protect yourself from a phishing attempt:

- **Double-Check:** If you're unsure about a message, call the organization using a number you know is real—not one provided in the message.
- **Change Passwords Regularly:** Be sure to change your passwords regularly and do not use the same passwords across multiple platforms.
- **Use Multi-Factor Authentication (MFA):** Adding an extra layer of security to your accounts can help keep them safe, even if someone gets your password.
- **Keep Everything Updated:** Make sure your devices have the latest software updates and security patches.
- **Trust Your Instincts:** If something doesn't feel right, it probably isn't. It's always better to be safe than sorry.

And remember, if you ever doubt the legitimacy of a communication you receive that claims to be from AB&T, please do not hesitate to contact us and verify. We are always available to ensure your financial security.

Together, we can make our digital world safer for everyone.

