People's BANK
We put people first.

Protect Yourself from Impersonation Fraud

Impersonation fraud happens when a scammer pretends to be someone you trust—such as your bank, a well-known company, or even a company executive—to trick you into sending money or sharing sensitive information.

These scams are increasingly common. Fraudsters may use fake phone numbers, emails, or websites that look legitimate, making it difficult to tell the difference at first glance.

HOW IMPERSONATION SCAMS WORK

Many impersonation scams follow a similar pattern:

- **Initial Contact:** You receive an unexpected phone call, text, or email that appears to come from a trusted organization. These messages often look very convincing, using familiar logos, professional language, and realistic email addresses or website designs.
- **Building Trust:** The scammer may claim to represent a well-known company or even pose as a high-level executive to appear credible and authoritative.
- **Creating Urgency:** You're told there's a problem—such as suspicious account activity—and that you must act immediately to prevent loss or resolve the issue.
- **Pressure to Act:** The scammer may threaten consequences or insist on secrecy, pushing you to act quickly without verifying the request. They may ask you to transfer money, share personal information, or download software.

WARNING SIGNS TO WATCH FOR

Be cautious if you notice any of the following:

- Unexpected calls, emails, or messages—especially from unfamiliar contacts
- Requests that create urgency or pressure you to act quickly
- Instructions to keep the situation secret
- Threats if you don't respond or comply
- Links or attachments that seem suspicious
- Email addresses or websites that look similar to legitimate ones, but with slight differences

HOW TO PROTECT YOURSELF

You can take simple steps to stay safe:

- **Pause before acting:** Take a moment to evaluate the request, especially if it feels urgent
- **Verify independently:** Contact the organization directly using a trusted phone number or website—not the contact details provided in the message
- **Avoid clicking unknown links:** Go directly to official websites instead

- **Protect your information:** Never share sensitive details unless you're certain of who you're communicating with

REMEMBER

Legitimate organizations will **never pressure you into immediate action**, demand secrecy, or request sensitive information in an unexpected or unsecured manner.

If something doesn't feel right, trust your instincts and take the time to verify.