Phishing Scams

Scammers use emails and websites that falsely claim to be from legitimate banks, financial institutions, or companies. Their goal is to manipulate you into disclosing personal and financial data.

Phishing attempts often involve fake emails or websites that mimic trusted sources, prompting you to click a link or enter sensitive information like passwords or credit card numbers. Scammers are also known to adapt their messages to current events, making their tactics even more convincing. These scams are designed to exploit your trust and create a sense of urgency by claiming your account is at risk.

Mid-States Organized Crime Information Center

Resist the pressure to act immediately. Scammers rely on creating a sense of urgency to make you act without thinking.

Take your time to assess the situation carefully.

Verify the identity of the caller or sender by asking questions that only the real person or organization would know.

Contact the agency or person directly using a trusted number or an official source.

Do not provide personal, financial, or account details to unsolicited callers, emails, or messages.

Sharing this information can lead to identity theft or financial fraud.

Do not send money through wire transfers, gift cards, or cryptocurrency.

Legitimate organizations will never ask for payment in these forms or demand immediate payments.

If you receive a suspicious call, end it immediately without providing any information.

Scammers rely on keeping you engaged, so hanging up is your best defense.

Notify the appropriate authorities, such as your local law enforcement agency, about the suspicious activity.

Reporting helps protect others from becoming victims and assists in tracking down scammers.

Share details of the scam with family, friends, and colleagues to raise awareness and prevent them from falling victim.

Spreading the word helps others recognize and avoid similar scams.