Phishing Prevention Guide

How to Spot and Avoid Online Scams

What is Phishing?

Phishing is when scammers pretend to be trusted organizations to trick you into sharing personal information. They might pose as:

- Your bank or credit card company
- Government agencies (IRS, Social Security)
- Tech companies (Microsoft, Apple)
- Online stores (Amazon, Walmart)
- Email providers (Gmail, Yahoo)
- Delivery services (UPS, FedEx)

Common Types of Phishing

1. **Email Phishing**: Fake emails that look like they're from legitimate companies
2. **SMS Phishing (Smishing)**: Text messages containing suspicious links
3. **Voice Phishing (Vishing)**: Phone calls from scammers pretending to be from legitimate organizations
4. **Website Phishing**: Fake websites that look identical to real ones

10 Warning Signs of Phishing

1. **Suspicious Sender Address**: Check the email address carefully, not just the display name
    - Example: amazon-support@secure-notice.com instead of support@amazon.com
2. **Generic Greeting**: "Dear Customer" instead of your actual name
3. **Urgent Language**: Claims that you must act immediately or face consequences
4. **Poor Grammar and Spelling**: Professional companies rarely make obvious mistakes
5. **Suspicious Links**: Hover (don't click) to see where links really lead
6. **Requests for Personal Information**: Legitimate organizations rarely ask for sensitive information via email or text
7. **Unexpected Attachments**: Be wary of attachments you weren't expecting

8. **"Too Good To Be True" Offers**: Unusual prizes or deals you didn't sign up for
9. **Threatening Language**: Warnings about account closure or legal action
10. **Unusual Payment Requests**: Asking for payment via gift cards, wire transfers, or cryptocurrency

How to Protect Yourself

DO:

- **Type website addresses** directly in your browser instead of clicking links
- **Call the organization directly** using the phone number from their official website (not from the email or call you received)
- **Use unique passwords** for all your important accounts
- **Keep your devices updated** with the latest security software
- **Enable two-factor authentication** for important accounts when available
- **Be skeptical of urgent requests** - take time to verify before responding

DON'T:

- **DON'T click links** in suspicious emails or text messages
- **DON'T download attachments** from unknown senders
- **DON'T share personal information** in response to an email or call you didn't initiate
- **DON'T trust caller ID** - it can be spoofed (faked)
- **DON'T make hasty decisions** when pressured - legitimate organizations give you time to think

What to Do If You Suspect Phishing

For Email:

1. Don't click any links or download attachments
2. Don't reply to the sender
3. Report it by forwarding to:
    - reportphishing@apwg.org (Anti-Phishing Working Group)
    - The company being impersonated (using their official contact info)
4. Delete the email

For Text Messages:

1. Don't click any links
2. Forward the message to 7726 (SPAM) to report it
3. Block the number and delete the message

For Phone Calls:

1. Hang up immediately
2. Don't call back using the number they provided
3. Find the official number and call that instead if you're concerned

If You've Already Responded to a Phishing Attempt:

1. **Change your passwords** immediately for any affected accounts
2. **Contact your bank or credit card company** if you shared financial information
3. **Monitor your accounts** closely for suspicious activity
4. **Place a fraud alert** on your credit reports by calling:
    - Equifax: 1-800-685-1111
    - Experian: 1-888-397-3742
    - TransUnion: 1-800-916-8800
5. **Report identity theft** at identitytheft.gov if your personal information was compromised

Remember:

- Being targeted is **not your fault** - scammers target everyone
- If something feels suspicious, trust your instincts
- When in doubt, verify through official channels before responding
- Legitimate organizations won't pressure you for immediate action

Help Others Stay Safe:

- Share this guide with friends and family
- Offer to be a "verification buddy" for others to consult when they receive suspicious messages
- Report scams to help protect your community

Created by Scam Not Me - Helping older adults stay safe online