Additional Resources

Credit Bureaus
Equifax
800-525-6285
www.equifax.com

Experian
888-397-3742
www.experian.com

TransUnion
800-680-7289
www.transuinion.com

Government Sites
Federal Trade Commission
www.ftc.gov

Department of Treasury
www.treasury.gov

Internet Crime Complaint Center
www.ic3.gov

Identity Resource Page
www.identitytheft.gov

Opt-out Services
Do Not Call Registry
www.donotcall.gov

Privacy Rights Clearinghouse
www.privacyrights.org

Prescreened Credit Card Offers
www.optoutpresreen.com

Your independently owned
ADVANTAGE®
PAYROLL SERVICES

A Guide of Best Practices

Bruce Patz - Owner
Advantage Payroll Services
(978) 637-2266
B.Patz@massadvantagepayroll.com

Protecting Your Information:

A Guide of Best Practices

Your independently owned
ADVANTAGE®
PAYROLL SERVICES

Identity Theft: How Identity is Stolen and How to Protect Yourself:

Methods for stealing identity:

* **Dumpster Diving**
  Rummaging through a person's trash looking for papers that include personal information

* **Phishing**
  Sending a user a fake email in an attempt to trick the user into providing personal information

* **Pretexting**
  Calling a person directly claiming that they have something to offer that would entice a person to disclose personal information

How to protect yourself:

* Do not throw documents away that can be used to identify you. Shred these types of documents.

* Protect online accounts with passwords difficult to guess. Avoid common identifiers such as date of birth, pet's name or mother's maiden name.

* If you receive a call at home or work, never give out any personal information over the phone. Either return a call or request something in writing be sent to your home address.

How to Protect Yourself from Phishing Scams

- Be wary of hyperlinks in email messages as they are constructed on the surface to look legitimate but underneath they often redirect you to a fraudulent website. Rather than click on a suspicious link, type the link into the browser window.

- Be alert to hyperlinks misspelled.

- Make sure to use anti-virus, anti-spam, anti-spyware and a personal firewall. These products should be updated regularly and kept current.

- Always scan file attachments for viruses or malicious software before opening them.

- Routinely review and apply software security patches to your computer operating system and applications.

- Choose secure passwords to protect account information. They should be at least eight characters in length with a combination of letters, numbers and special characters and should not be easily guessable.

- Avoid responding to emails that do not come from someone you know. If an email comes from someone you know, but you were not expecting it or it seems suspicious, contact the sender to confirm that they sent it prior to responding.

Phishing Red Flags—Common Techniques

Urgent emails or threats to accounts
Email claims the recipient's account has been accessed and request authentication information such as usernames and passwords**.**

Lost information
Consumers should be cautious of claims that a company is "updating" its files or accounts.

Personal information request
Requests made for a recipient to enter personal information, click on a link or completing an email form should be treated with suspicion.

Senders address
Email recipients should not solely rely on the email sender's address to validate true origin. The "From" field of an email can easily be altered.

Links in emails can be easily forged
Links on emails can be misleading, luring recipients to a forged version of a legitimate website.

Other signs of a phishing email
Other telltale signs of phishing emails include spelling errors, incorrect grammar, pop-up windows that look like sign in pages and unsuspected attachments that may contain a virus or malware.