Foiling IDENTITY THEFT

- IT'S A -
MONEY THING®

SHRED IT!

Not all identity theft starts online. Trash cans and recycling bins are still an easy way for thieves to access your personal information.

A personal shredder ($20–$30 for a basic model) is a small investment that makes a huge difference.

Not sure what to shred? Here are some examples:

- *Addressed envelopes*
- *Bank statements*
- *ATM receipts*
- *Expired credit cards*
- *Cellphone bills*
- *Utility bills*
- *Old boarding passes*
- *Email printouts*
- *School schedules*
- *Old report cards*
- *Travel itineraries*
- *Old store credit cards*
- *Paycheck stubs*
- *Resumés*
- *Pre-approved credit card offers*
- *Receipts*
- *Canceled or voided checks*
- *Magazine address labels*

IDENTITY THEFT AND SOCIAL MEDIA

Is your hometown and relationship status publicly listed on your Facebook profile?	**Do your online usernames contain numbers relating to your age or the year you were born?**	**Can others tell when you're out of the house or out of town based on your Instagram feed?**

If you answered yes to any of these questions, **you're making it easier for identity thieves** to take advantage of your information.

Vary your passwords, customize your privacy settings and think before you share that next status update or photo.

WHAT ARE THE WARNING SIGNS?

- Unexpected withdrawals or charges listed in your bank or credit card statements
- Errors in your credit report
- Missing mail
- Receiving unexpected bills and credit cards by mail
- Problems accessing your email or online banking accounts
- Calls from debt collectors regarding accounts that are not yours
- Issues with medical insurance or inaccuracies in your health records
- Receiving a notice from the government that multiple tax returns were filed in your name

Did you know there's an entire Twitter account devoted to retweeting photos that people have posted of their credit and debit cards?

No matter how excited you are about your new card, **never share it online.**

BROUGHT TO YOU BY

Dupaco

How to Spot SCAMS

IT'S A MONEY THING®

EMAIL PHISHING SCAMS

Do you know how to spot them? This example and the tips below will help you recognize a suspicious email.

Email

Inbox (9)
Sent
Drafts
Spam
Trash

ACTION required or your account will be DELETED 1

Joe Shabadoo <jshabadoo@grnail.com> 2 Jan 26 at 3:29 AM 3

Valued Customer, 4

Someone has gained unauthorized access to your account. Reset your Pass Word imediately. 5

RESET PASSWORD 6

Customer Support: http://youraccount.com/dcijflksd%al
Questions? Contact: 1-800-555-3942 7

View Attachment: Status_Report.doc.file 8

KEEP AN EYE OUT FOR THESE RED FLAGS

1. **The subject line** Scammers tend to use an urgent or aggressive tone.
2. **The sender** In the example above, is the sender using a Gmail address? If you said yes, take a closer look! It's actually g-r-n-a-i-l.com. Sneaky scammers will use email handles that are one letter off from what they should be (e.g., "netftix" instead of "netflix") so that, at a glance, everything appears official.
3. **The time stamp** When was the email sent? This is an especially telling clue when a scammer is impersonating someone you know or correspond with regularly.
4. **The greeting** Does it address you by name, by email address or by a generic title? A generic or awkwardly phrased greeting could be the sign of a scam.
5. **The spelling** Errors in spelling and grammar are always a red flag.
6. **Buttons and links** These are easy for scammers to format and disguise. Get in the habit of accessing your accounts by typing the official URL in a new browser window. Avoid using the direct links in your email messages.
7. **The contact info** Does it look sketchy? If you need to verify the legitimacy of the sender, never use the contact information contained within the email. Cross-reference it with a separate web search.
8. **Attachments** Malicious files can be easily disguised as innocent Word documents, spreadsheets and presentations. Be deliberate about which attachments you choose to open or download.

REPORTING EMAIL SCAMS

Email phishing attempts (even the unsuccessful ones) can be reported here:

Internet Crime Complaint Center (IC3)
www.ic3.gov

Federal Trade Commission (FTC)
www.FTC.gov/complaint

BROUGHT TO YOU BY

Dupaco