



IF IT SMELLS "PHISHY," IT PROBABLY IS.
HELP KEEP YOUR IDENTITY SAFE AND SECURE.



HELP KEEP YOUR IDENTITY
SAFE AND SECURE FROM PHISHERS.



Phishing (pronounced "fishing") has become a great threat to consumers. Done via e-mail or, less commonly, over the phone, phishing is when thieves trick people into providing their Social Security numbers, financial account numbers, PINs and other personal information. Phishers often appear legitimate by accurately imitating official Web sites, e-mail templates or phone calls — so it's important to know what to look for.

Watch for these signs

- E-mails or phone calls reporting problems with one of your accounts that ask you to confirm your personal information.
- Threats that your account could be closed or canceled.
- Phishers posing as employers who found your name on a job search site.

Here's how you can protect yourself

- Be suspicious if someone contacts you unexpectedly and asks for your personal information. It's a warning sign that something is "phishy." Most legitimate companies don't operate that way.
- Don't click on links in e-mails that ask you to provide personal information. To check

PHISHING IS BECOMING MORE
PREVALENT EVERY DAY.
BY TAKING THESE PRECAUTIONS
AND BEING AWARE, YOU
CAN HELP STOP IT.

whether an e-mail or call is really from the company or agency, call it directly or go to the company's Web site (use a search engine to find it).

- Job seekers should verify the identity of someone claiming to be a prospective employer before providing them with personal information.