Top Ten Imposter Scams

Scammers are all over the Internet just waiting to prey on unsuspecting individuals who are willing to give up their personal information. The FTC recently released the following listing of the top ten imposter scams for 2014:

1. IRS Imposters. The real IRS won’t initiate contact by e-mail or phone, they will start with a postal letter.
2. Surprise? A Prize Patrol contacts you about winning a large sum of money; only thing is you need to send them some money to collect your prize. Don’t believe it.
3. PCs R Us. Someone contacts you to inform you that your computer has a serious technical problem which they can solve for you. Not true.
4. Mal-Where? Someone calls pretending to be from Microsoft or other Technical Support and says there is dangerous software on your machine. Just click on the pop-up that may be on your screen. Don’t.
5. Fake Fed. Similar to the old Nigerian e-mail scam, only now a fake federal agent is confirming that Nigerian royalty really does want your help to move a large sum of money out of their country.
6. Kidnapped Computer. You click on a link and a pop-up appears saying you have been locked out of your files. Don’t pay the ransom to unlock your files; more often than not even if you pay, the files won’t get unlocked. Tip, remember to back up important files often.
7. Government Grants. Someone posing as a federal official tells you that you have won a government grant, really? All you need to do is pay associated taxes and fees and you will be sent the money.
8. Medicare Disqualification. A bogus government representative claims to work for Medicare or for the Affordable Health Care Act and you will lose benefits unless you pay a fee or provide updated personal information.
9. Deportation. A variation on the bogus government representative is a caller from Homeland Security who threatens an immigrant with deportation notices, but will help to ‘certify’ them for a fee and/or by providing updated personal information.
10. Caller ID. A scam that spoofs caller ID in order to get you to pick up the call. In some cases this incurs usage charges.

Avoid being a victim -

- Be suspicious of unsolicited phone calls, visits, or email messages asking about internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don’t send sensitive information over the Internet before checking a website’s security.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.
- Take advantage of any anti-phishing features offered by your email client and web browser.