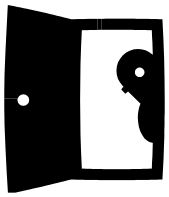
Practical Help Tip Sheet:

#002: Don't fall for scams! (v1.0)

Tip #1: Scammers and hackers are creative artists These bad guys use social engineering to fool you into letting them hack into your home, workplace or computer. They are constantly creating new ways to fool you, so you need to be wary – don't fall for these scams. Here are some tried-and-true ways they try to get into your workplace:

1. You're walking in the front door and someone's right behind you, maybe with arms full of packages. They ask you to hold the door for them.
2. Someone ahead of you is impatient and acting frustrated because they need to get inside your building and the guard won't let them in without a pass. They get more and more upset until the guard gives in or someone else 'vouches' for them without even knowing them.
3. Someone's hanging around an outside designated smoking area. As workers come and go, they just follow one inside.



Tip #2 For getting into your home, here are some of the most common ways:

1. A broken-down car, can they use your phone?
2. Can they use your bathroom?
3. They are conducting a survey or offering something, can they come inside?
4. They say your neighbor sent them over with something for you.

Once inside, they find creative ways to get into your computer, such as:

Tip #3 In the workplace:

1. Someone comes into your cubicle or office saying they're from IT and need to update or check your computer. They may even have a company badge. This could also just be a phone call where they ask you to give them remote access.
2. Someone comes in and asks to test or fix something under your desk, like a plug. While there, they put a little device between your keyboard and your computer to record your keystrokes.

Tip #4 At home or at a public place:

1. Their phone/laptop is dead, can they borrow yours to make a call/check a quick website?
2. They can see you type from over your shoulder!
3. They can listen to what you are saying, too!

Tip #5 Social engineering can also take advantage of your trust in email or social networking websites. For instance:

1. You get an email from someone you know (at least by the email address), saying they're trapped somewhere and asking you to send them money.
2. You get an email asking if you've seen something online about you (a blog, news story, etc.). Of course the link is fake.
3. You get an email with a link from a business or bank asking you to click and log into your account.
4. You get an email, phone call or door-knocker asking for donations to help a worthy cause (like last year's Hurricane Sandy relief). Or with free gift or gift card offers.
5. You see a post on Twitter or Facebook with a shortened link, like the popular bit.ly. Who knows where that link will take you.

Tip #6 Faking Email is Easy You need to know that anyone can send an email that looks like it comes from anyone else. It's ridiculous that emails can be so easily faked. Social networking sites are a little harder to fake, but it's certainly do-able. And anyone can knock on your door with papers or identification that they ginned up themselves. I'm sad for the legitimate non-profits, but there are just too many scammers out there these days.