

Turn Awareness Into Action...

Beware Of "Social Engineers"

Who are social engineers? Social engineers are individuals who use lies and deception to gain access to protected health information (PHI) they are not authorized to have. *Social engineers depend on your goodwill and try to earn your trust. They rely on your desire to be helpful and hope that you will not challenge their identity or authority.*

What do they do? Social engineers may (1) send an email that tricks you into sharing your password and other personal information so they can commit identity theft, (2) try to persuade you into sharing confidential information over the phone or in person, or (3) walk into your work area posing as an IS support person and ask for your UserID and password to gain access to your computer so that they can "fix" a problem.

Here are things you can do to prevent being "victimized" by Social Engineers:

1. Never open/forward email or attached files from unknown senders. Immediately delete email that looks suspicious.
2. Be suspicious of unfamiliar phone calls or visitors. Verify an individual's identity and authority before disclosing PHI.
3. Do not allow individuals without proper UCMC ID Badges to gain access into the Medical Center or a secured room with your swiped ID Badge (Piggybacking). Politely ask them to show their ID Badge or help escort them to a security officer.
4. Get to know your IS support staff and their procedures. Do not give out your password and never store it near your computer.

Suspicious that someone is a "social engineer?"

Who are you going to call? The HIPAA Program Office at 4-9716.

Be Ready...

Do Not Fall For Social Engineering