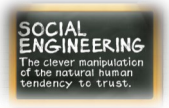
SECURITY AWARENESS NEWSLETTER

Technology and Communications **JUNE 2018**

What is Social Engineering?



Social engineering is a psychological attack where an attacker tricks you into performing actions or giving confidential information. Cyber criminals can use publicly-available information to trick you into divulging passwords or providing them access to restricted information and areas. These attacks can be done in person, or through remote means such as over the phone and email. These efforts are designed to manipulate you by playing on your natural tendency to trust. Also, be wary of what you post on social media. Cyber criminals can learn your habits and use the information gained to trick you and/or earn your trust.

Types of Social Engineering Attacks - Here's what to look out for.

Phishing - You receive an email from someone pretending to work for a reputable company, such as your job or your bank. These emails ask you to submit information that the organization should already have. Many times cyber attackers may masquerade as your boss, or someone who works with you in your organization, such as IT, and attempts to get you to give them information, access, or even money. They may also send you links that direct you to malicious sites that look like the real thing.

Tailgating - An attacker may follow employees or personnel after they key or badge into restricted areas. These attackers can pose a physical security risk as well.

Baiting - Hackers may attempt to insert malicious code into files that appear legitimate and harmless. Be wary of ALL attachments and links. Music files, movie downloads, and Microsoft Office documents are usual suspects. These files can have generic general sounding names such as "Quarterly Earnings Statement" or "2017 Tax Return." These names are designed to grab your attention and lower your guard, ultimately subjecting you to cyber attack.

Detecting/Stopping Social Engineering Attacks - Learn how to protect yourself.

Fortunately, stopping such attacks is simpler than you may think. Common sense is your best defense. If something seems suspicious or does not feel right, it may be an attack. The most common clues of a social engineering attack include:

- Someone creating a tremendous sense of urgency. They are attempting to panic and fool you into making a mistake.
- Someone asking for information they should not have access to or should already know, such as your account numbers.
- Someone asking for your password. No legitimate organization will ever ask you for that.
- Someone pressuring you to bypass or ignore security processes or procedures.
- Something too good to be true. For example, you are notified you won the lottery or an iPad, even though you've never played.
- Someone you do not recognize is in a restricted area. Report suspicious activity to security.

To protect yourself and the organization, always verify such requests by reaching out to the sender using a different communications method, such as in person or over the phone. If you suspect someone is trying to trick or fool you, do not communicate with the person anymore. If the attack is work-related, be sure to report it to the Service Desk immediately. Remember, you have to be right every time. The bad guys only have to be right once. Stay vigilant!

Technology and Communications Department
Help@albanyga.gov
(229) 438-3988

CITY OF Albany GEORGIA