1. Computer Security

Computer security, also known as cyber security or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.

The field is of growing importance due to the increasing reliance on computer systems and the Internet in most societies, wireless networks such as Bluetooth and Wi-Fi - and the growth of "smart" devices, including smartphones, televisions and tiny devices as part of the Internet of Things.

计算机安全是计算机与网络领域的信息安全的一个分支。其目的是在保证信息和财产可被受权用户正常获取和使用的情况下,保护此信息和财产不受偷窃,污染,自然灾害等的损坏。计算机系统安全是指一系列包含敏感和有价值的信息和服务的进程和机制,不被未得到授权和不被信任的个人，团体或事件公开，修改或损坏。由于它的目的在于防止不需要的行为发生而非使得某些行为发生，其策略和方法常常与其他大多数的计算机技术不同。

2. Computer Attack

In computer and computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

于电脑和电脑网络中，破坏、揭露、修改、使软件或服务失去功能、在没有得到授权的情况下偷取或访问任何电脑的数据，都会被视为于电脑和电脑网络中的攻击。

3. "Social engineering" means using human to human contact, say on the phone, to get into a system. Some people can be quite persuasive on the phone, and most people are polite and helpful by default. A bad guy might pose as technician showing up, trying to fix the printer. People will often be polite to a well-dressed person on site who appears to be doing something proper.

4. Phishing Attacks

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

钓鱼式攻击是一种企图从电子通信中，通过伪装成信誉卓著的法人媒体以获得如用户名、密码和信用卡明细等个人敏感信息的犯罪诈骗过程。

5. Malware Attacks

Malware, short for malicious software, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

恶意软件，是形容网络上散播的如同“流氓”一样讨厌的软件。采用多种社会和技术手段，强行或者秘密安装，并抵制卸载；强行修改用户软件设置，如浏览器的主页，软件自动启动选项，安全选项；强行弹出广告，或者其他干扰用户、占用系统资源行为；有侵害用户信息和财产安全的潜在因素或者隐患；与电脑病毒联合侵入用户电脑；停用杀毒软件或其他电脑管理程序来做进一步的破坏；未经用户许可，或者利用用户疏忽，或者利用用户缺乏相关知识，秘密收集用户个人信息、秘密和隐私；恶意篡改注册表信息；威胁恐吓或误导用户安装其他的产品。

6. Private Key Cryptography

Symmetric-key cryptography uses the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption).

对称密钥加密，又称为对称加密、私钥加密、共享密钥加密，是密码学中的一类加密算法。这类算法在加密和解密时使用相同的密钥，或是使用两个可以简单地相互推算的密钥。实务上，这组密钥成为在两个或多个成员间的共同秘密，以便维持专属的通讯联系。与公开密钥加密相比，要求双方取得相同的密钥是对称密钥加密的主要缺点之一。

In cryptography, a private key is a variable that is used with an algorithm to encrypt and decrypt code. Quality encryption always follows a fundamental rule: the algorithm doesn't need to be kept secret, but the key does. Private keys play important roles in both symmetric and asymmetric cryptography.

7. Public Key Cryptography

Public-key cryptography, or asymmetric cryptography, is any cryptographic system that uses pairs of keys: public keys that may be disseminated widely paired with private keys which are known only to the owner. There are two functions that can be achieved: using a public key to authenticate that a message originated with a holder of the paired private key; or encrypting a message with a public key to ensure that only the holder of the paired private key can decrypt it.

公开密钥加密，也称为非对称加密，一种密码学算法类型，在这种密码学方法中，需要一对密钥，一个是私人密钥，另一个则是公开密钥。这两个密钥是数学相关，用某用户密钥加密后所得的信息，只能用该用户的解密密钥才能解密。如果知道了其中一个，并不能计算出另外一个。因此如果公开了一对密钥中的一个，并不会危害到另外一个的秘密性质。称公开的密钥为公钥；不公开的密钥为私钥。

In cryptography, a public key is a value provided by a designated authority as an encryption key. A system for using public keys is called a public key infrastructure (PKI). The Public-Key Cryptography Standards (PKCS) are a set of intervendor standard protocols for making possible secure information exchange on the Internet using a public key infrastructure (PKI).