سلامة
SALAMA
شركة سلامة للتأمين التعاوني
Salama Cooperative Insurance Company

CYBERSECURITY
DEPARTMENT

Definitions Of The Week

Dear all;

1. **Malware- Any piece of software that was written with the intent of doing harm to data, devices or to people.**

2. **Trojans- A malware that disguises itself as a legitimate software. “Acts discretely and creates backdoors in your security to let other malware in”.**

3. **Adware- Software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online.**

4. **Spam- irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing and spreading malware.**

5. **Ransomware- this malwares intent is to hijacks files encrypts them, and demands money from the victim in exchange for a decryption key**

SALAMTEQ
Cybersecurity Dept.

سلامة
SALAMA
شركة سلامة للتأمين التعاوني
Salama Cooperative Insurance Company

CYBERSECURITY
DEPARTMENT

Mobile Security Tips

SALAMTEQ
Cybersecurity Dept.

Dear all;

1. Create a strong password. Avoid using very common password ideas, such as your birth date, your middle name or your pet's name. Instead, create something random but rememberable. Also, use alphanumeric combinations whenever possible.

2. Don't trust messages that attempt to get you to reveal any personal information. Treat messages the same way you would treat email, always think before you click! Smishing (phishing via SMS)

3. Only use apps available in your device's official store - NEVER download from a browser. Be wary of apps from unknown developers or those with limited/bad reviews. Keep them updated to ensure they have the latest security.

4. Be wary of any Social Media links you receive on your phone as well. Many times, these can be used to install malware on your mobile device in order to steal personal information.

5. Always be on the lookout for https:// websites while doing online transactions of any kind. These sites offer a connection secure enough to ensure that no third parties can see the information you enter on these sites.

6. Never use a public or unknown Wi-Fi internet connection to work on your sensitive data in mobile application. Even someone who doesn't have experience in programming can instantly connect to your tablet or phone and steal information from it!

7. Don't click on the links you receive through email - not even if the sender appears like a legitimate one. Hackers can create logos, emails and even entire websites that look the same as well-known companies - and thus, they can attract users into unknowingly sharing their passwords with them.

8. Update your mobile phone's operating system. The more recent your OS version is, the more protected you will be.

salamacic
www.salama.com.sa/

سلامة
SALAMA
شركة سلامة للتأمين التعاوني
Salama Cooperative Insurance Company

CYBERSECURITY
DEPARTMENT

Ransomware

Dear all;

Beware of a malicious software that locks a device, computer, tablet or smartphone and demands a ransom to unlock it.

First attempt for this attack was in 1989, 2017's Biggest Cyber attack: The biggest ransomware attacks are Wannacry and Petya.

Common ransomware variants
- **WannaCry: Targets windows OS by encrypting systems data and file.**
- **Killdisk : Deletes hard drive data completely.**
- **Locky: Microsoft Word document that contains malicious code that will encrypt all files.**

What to do:
- **Back up data regularly**
- **Block and filter suspicious email**
- **Educate users on safe email and file use**

SALAMTEQ
Cybersecurity Dept.

salamacic
www.salama.com.sa/

سلامة
SALAMA
شركة سلامة للتأمين التعاوني
Salama Cooperative Insurance Company

CYBERSECURITY
DEPARTMENT

Social Engineering

Dear all;

The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Common Social engineering attack:

In-person: Using personal skills to gather information

-Interview the victim
-Speaking with victim on the phone
-Keep an eye on his personality & habit

Digital: Using technology to gather information

-Phishing: friendly email or SMS
-Fake adv
-Typo squatting

Info Social media knows about you:

Name
Family Name
Mobile
Email
Photos
Video
Location information
Birthday
Credit Card Information
Mailing Address
Hardware Setting
Device Setting

What this Info could be used for:

-Identity theft
-Password cracking
-Money stealing

SALAMTEQ
Cybersecurity Dept.

salamacic
www.salama.com.sa/