Language Services associates

www.lsaweb.com

Security Awareness

Security Threats

The 2 main security threats are:

Non-Physical Social Engineering

and

Physical Social Engineering

Non-Physical Social Engineering

- **Non-Physical Social Engineering** - Using the phone or internet in attempts to obtain valuable information, steal money, or to fulfill a personal agenda.
- **Common forms of non-physical social engineering:**

  Impersonation (phone) - Pretending to be someone else to trick the victim into revealing information or to perform an action.
  Spoofing - Virtual impersonation, done by falsifying the origin of the communication to mislead victims.
  Phishing - Fake emails and websites designed to look real to obtain valuable information.
  Baiting - Luring a person to perform an act for an empty-promise of a reward.

- A non-physical attack includes a sense of urgency, authority, name dropping and questionable details.
- To prevent an attack you should take your time and verify the identity and legitimacy of any unexpected requests.

PHYSICAL Social Engineering

- **Physical Social Engineering** - When a person or team physically attempts to gain access to confidential information or to fulfill a personal agenda.
- Physical social engineering is usually done by impersonating someone else to gain trust and entry.
- An attacker can be anyone.
- Most attacks are done to obtain valuable information, cause chaos, or other personal reasons.
- To prevent attacks, you should:
  - Look for badges on employees you do not know.
  - Be aware of tailgaters and any suspicious behavior from a stranger.
  - Report any suspicious activities to security immediately.

Goals of Physical Social Engineering

Goals of physical social engineering attacks include:

- Obtaining confidential information for financial gains
- Sabotage or expose a person or company's reputation
- To cause damage
- Personal reasons

Security is Everyone's Responsibility

- Under the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) you are responsible to safeguard the Protected Health Information (PHI) of the clients and end users for whom you provide interpretation services.
- LSA safeguards its systems to monitor for potential breaches in security.
- You must remain aware and diligent to avoid becoming a victim of social engineering attacks
- Always report any suspicious activity or potential breaches

Safeguarding Your Login is Vital

- A strong password is one of the best methods of defense.
- A strong password should be 8 or more characters in length, contain upper and lowercase letters, numbers and at least 1 special character.
- You should change your password at least every 30 days.
- You may change your password at any time, and must change it immediately if you think it may have been breached.
- Never share your password.
- Never write down your password.

Always lock your computer

Locking your computer is easy and can be done faster than standing up from your seat.

Simply press the **Windows Key + L**, and your computer will be locked.

It is that simple. Just remember to do it every time before you get up.

Proper Handling of PHI & PII

- You should avoid emailing PHI (Protected Health Information) and PII (Personally Identifiable Information).
- If you must email information containing PHI or PII you must use **secure email** to protect it from hackers.
- You should never type PII or PHI in the notes section of the interpreting platform.
- If you must take notes that contain PII, PHI or other confidential information, all notes must be properly destroyed (not in a trash can) at the conclusion of the interpretation.
- Never text PHI or PII as texts are not a secure transmittal system.
- Recording of any LSA calls/interpretation sessions is **strictly prohibited**. This includes over the phone, video remote and on location interpretation.

Compliance Concerns?
Contact LSA

Compliance concerns, questions, and more,

Give us a call when you're not sure!

Dial 833-234-4831

To voice your concerns as a compliance hero!

No need for your name, your phone number, or more,

Just leave us a message and we will explore!

Do the right thing,

Just give us a ring!

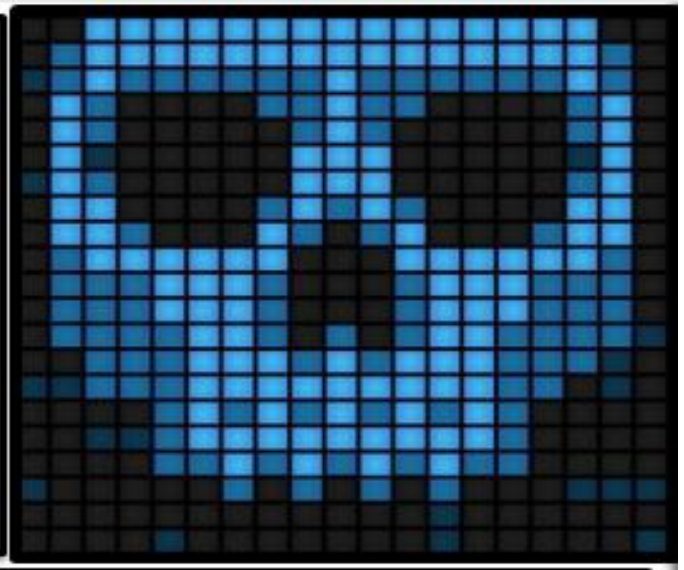
833-234-4831

Network/Wifi Usage

- Public networks are free wireless internet connections offered at public places such as coffee houses, restaurants and other institutions.
- Public networks are not as safe as you think they are. Refrain from doing work when you are connected to a public network.
- You must secure your home network if you are planning on using it for work.

Malware

Malware is short for **Malicious Software**. It is possibly **the most common threat to computer information security.**



Many malware are created by cyber criminals and social engineers to gain access or destroy information stored on computers. This means that personal and confidential information can be stolen, corrupted, or deleted.

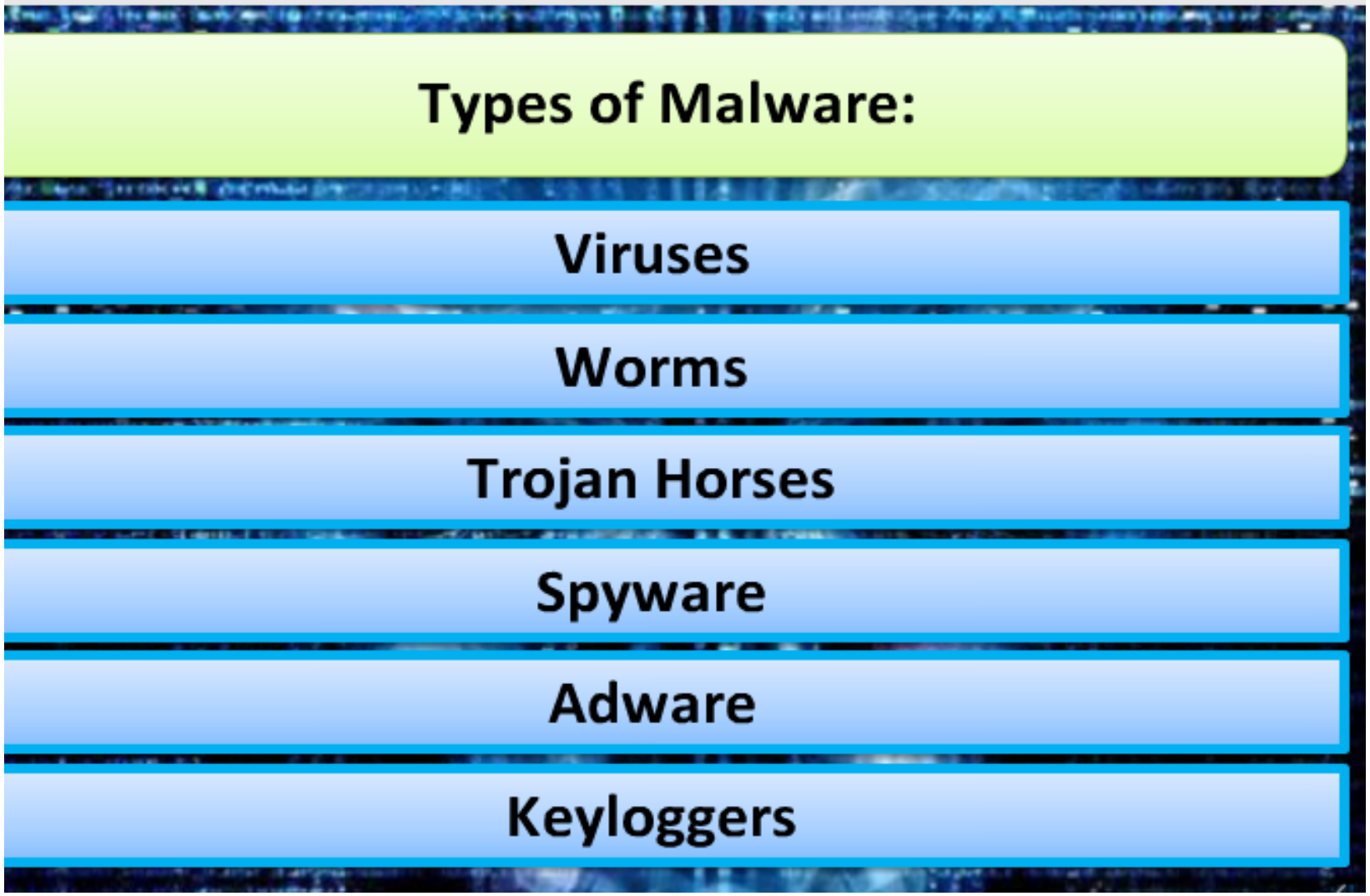
How can Malware affect you?

Malware can infect your computer in a variety of ways. In most cases, people will not be aware that they have been infected.

Here are the most common ways malware can infect your computer:

- You click a link that automatically installs malware on your computer.
- You visit an infected website that will install malware in the background.
- You open up an email attachment that automatically installs malware.
- You download and install software you assumed is safe but it contains malware.
- You click an advertisement that sends you to an infected website with malware.

Types of Malware



How to prevent Malware infections

Here are some guidelines to prevent infections:

- Do not click links from sources you do not know. Even if you know the source, be careful of the links you click, your friend or co-worker may have just been hacked or spoofed.
- Do not open attachments you are not expecting.
- Do not install software you do not know anything about.
- Do not run .exe (executable) files without knowing what it is first.
- Be careful clicking advertisements that seem too good to be true.
- Refrain from going to suspicious or dubious websites, these sites have a higher chance of containing malware.

Physical Security

- You should follow a Clean Desk Policy in your workspace by minimizing clutter, locking up all sensitive documents, and shredding all unneeded documents.
- Be mindful of the resources you use at work.
- You should always secure your personal and the company's property.
- Be aware of theft and report all incidents to security.
- When using shared work areas, make sure to not leave behind any sensitive information before departing.
- You should always be aware of your surroundings when out in public areas.
- Refrain from discussing and doing work on sensitive topics when you are out in public.

Questions?

- If you have any questions or concerns please contact LSA's Compliance Department Jbralow@lsaweb.com