Vermilion County, Illinois
Computer Use & Cyber-Security ALERT

02/08/2022

Introduction:

As is obvious from news reports nationwide, businesses and governments are at risk from cyber-attacks from hacking to ransomware attacks. Our County has been affected from time to time, and the types of threats and their frequency is rising fast. As a County, we need to re-think some of our policies and practices and will soon be working on a new technology and email section in our Personnel Policy. Pending that, we wanted to bring up some common issues that can lead to a complete loss of our ability to function and also our records. It is that serious. We all need to be more aware of the possibility of an attack and how we can prevent it. While this is an advisory memo for now, it may soon be the basis of an amended policy after review by the County Board.

Vermilion County is making every effort to provide its offices, officers and employees with the best and most secure technology available to conduct the County's official business. In this regard, the County has installed a County-wide network system, at substantial expense, to conduct its official business.

This document was created to advise all County users regarding the access to and the disclosure of information created, transmitted, received and stored via the use of the Internet, County e-mail, tablets, cell phones, computers and other electronic devices. We are providing an alert/advisory on some practices that can invite a cyber-attack. We request you follow this set of guidelines to prevent immediate harm.

The following requires strict adherence to protect the County's information and prevent potential loss of data due to computer viruses, malware, spyware, and/or ransomware. Employees should expect that a violation of these guidelines will result in disciplinary action, up to and including termination, when it is found that their actions, either intentional or by their negligence results in damages to the county system or equipment.

County Equipment

There is a constant threat of outside cyber-attacks and security breaches on the County's network information. All employees must be aware of this threat and use safe practices to minimize and reduce the risks to the County's computers and data.

- Therefore, absolutely no computer hardware or software should be installed on the County's network unless the Technology Services Department is consulted. (This includes but is not limited to computers, laptops, wireless access devices, etc.)

- Those who need to use a private laptop or computer must consult with the Technology Services Department to discuss the safety issues and risks involved before connecting the equipment to the County's network. Technology Services is not expected to fix, repair or install software, (including County anti-virus software) on any non-County owned computer or laptop.

- No County computer (or personal computer/laptop connected to the county network) is to be used to download games, unauthorized programs, movies, music or pornography, nor should any such items be loaded on a County computer from any source.

- No outside vendor should be allowed access to County computers, servers or the County internet services without consulting with the Technology Services Department (unless they have been pre-approved by Technology Services).

    - There are some vendors that need to frequently connect to an individual's pc to research problems (Example: Tyler/New World, Jano, DevNet property tax system).

    - These pre-approved vendors will not need to be approved each time they need access to a pc or server.

- Departments must not disclose wireless access point passwords to non-County employees without consulting with the Technology Services Department. In some departments, the wireless access points have been setup for public access use which limits access to and protects the County's network.

- Employees are assigned a user account and password to gain access to their pcs, laptops, e-mail accounts and specific system access. Each employee must keep their individual password information private.

- Employees are not allowed to use another individual's user account and password. This includes accessing computers, e-mail, tablets, phones and access to all programs (Tyler New World, Jano, Devnet, google, etc.).

- Individuals should NOT power down their pcs at the end of the work day. There are programs that run nightly to scan the pc and install various security updates. These updates and scans cannot run if the pc is powered down. (The scans and updates will eventually run when the pc is powered up but will slow down the pc during normal business hours.)

- An individual must lock or log off of their pc at the end of the business day to prevent another person from using their pc.

- Each individual is advised to regularly backup files on their pcs that are not currently saved to a County server. They must use a USB or thumb drive that has not been used for other purposes. (County servers are backed up nightly but the individual pc files are not automatically saved).

- Each individual or office must contact Tech Services <u>immediately</u> if they suspect any kind of threat to their computer or e-mail.

Internet

Access to the Internet is provided to County offices and employees for the purpose of conducting official County business. (Official County business refers to any duty, function or responsibility that is required by a County department.) The internet may not be used for prohibited purposes, such as conducting private business, or any other illegal use.

Internet Usage

- The department head or elected official will determine if an employee is allowed to use the internet for non-county business.

- When an employee accesses the internet, they must follow County guidelines on what they can access on the internet. (For example, they are not allowed to download games, unauthorized programs, movies, music or pornography). Opening such sites can risk the security of your office's files as noted below.

- County equipment cannot be used for personal gain or to conduct private business.

- Employees must be aware that certain aspects of the internet are forbidden and may put the County at risk to downloading viruses. The County's network, computer systems and bandwidth are expensive and limited. These resources are to be used for conducting official County business only. Therefore, employees must NOT use the internet for entertainment. This includes but is not limited to: streaming live music, videos, sporting events, tv shows, downloading screen-savers, games, gambling, etc.

- The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited. These can invite cyber-attacks.

- Never download a file or install a program from the internet without permission from Technology Services. You could be introducing a virus or other malware to our system.

- Resources of any kind, for which there is a fee, must not be accessed or downloaded without prior approval from a supervisor. This could be an attempt to gain financial information or a phishing attempt.

Data & Confidentiality

For all employees who may have access to confidential information.

Confidential and proprietary information is secret, valuable and expensive. Hackers are constantly searching for ways to obtain confidential information. If we leave the door open by accessing outside sites, we could expose this information. Common examples of confidential information are:

- Unpublished financial information (Ex: bank account routing numbers).
- Data of customers/partners/vendors.
- Confidential Customer information (social security number, birth dates, driver's license numbers, credit card information, etc.).
- Documents and processes explicitly marked as confidential.

Departments should:

- Train their employees on privacy and security measures.
- Establish clear procedures for reporting privacy breaches or data misuse.
- Establish data protection practices (document shredding, secure locks, frequent backups, access authorization, etc.).

Employees should always:

- Lock or secure confidential information at all times.
- Shred confidential documents when they are no longer needed (per department policy).
- View confidential information on secure devices.
- Only disclose information to other employees when it is necessary to their position and authorized.
- Keep confidential documents inside the department unless it is absolutely necessary to move them.
- Keep their passwords private and secure.

Employees must never:

- Disclose confidential information to unauthorized personnel.
- Replicate confidential documents and files and store them on insecure devices.

Precautionary Measures

- A department may ask an employee to sign a non-disclosure agreement (NDA).
- Whenever possible, electronic data must be stored on a server so it can be backed up periodically.

E-Mail:

- E-mail is not private communication. All information transmitted via internet/e-mail can be reviewed at any time.
- The use of County e-mail is restricted to official County business. County e-mails may not be used for private business, or any other non-county use. Again, this may open the County system to virus' or other attacks.
- E-Mail passwords are to be kept private. Each employee must maintain secure passwords and never use an account assigned to another user. Once a hacker gets ahold of your password, the County is at jeopardy. (Department heads may maintain a list of their employee passwords as needed.)
- Chain letters are illegal and may not be transmitted through e-mail.
- The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited. These can invite cyber attacks aside from being improper unless you are a law enforcement officer or investigator.
- Never send, post or provide access to any unauthorized confidential County materials or information.
- Do NOT open e-mails from unknown or suspicious sources.
- Do NOT open e-mail attachments that are suspicious. This can include an attachment from an unknown sender or an attachment that is not expected.
- If an employee has opened a suspicious e-mail or e-mail attachment, they must immediately contact the Technology Services Department to investigate if a virus has been downloaded or installed on the pc.