CYBER SECURITY newsletter

IT STAFF

Problem

Highly sophisticated threats are targeting our sensitive information. One of the most effective ways to compromise that information is to target the very people who maintain it, you. As a matter of fact, IT Staff are a primary target due to the privileged access you have to our systems and information. Cyber attackers will harvest information about our organization through resources such as our website, Facebook and LinkedIn, identify key employees such as yourself, then launch attacks specifically against you. However, as IT Staff you are also a powerful weapon, you are one of our best resources for protecting against these advanced attacks.

Solution

First, remember that you have privileged access to highly sensitive systems. As a result, your authentication credentials must be well protected.

Always log into a system with your unique user id, then elevate your privileges to administrator, root or any other privileged account. Never log in directly as a privileged user. Also, never share your login or password with others, including a supervisor. If they have access to your password, not only can they bypass our security controls but you will be responsible for any of their actions. Finally, never use the same password for a work related account as you do for any personal accounts, such as Facebook or your personal email accounts.

As an IT Staff member, at times you may need to discuss technical issues with individuals who do not belong to our organization. Please use the following guidance whenever discussing technical details about our organization.

IT Staff

IT Staff are a primary target due to the privileged access you have to our systems and information. However, as IT Staff you are also a power weapon in protecting against these attacks. Learn how you can help protect yourself and our organization.

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

You Are a Human Sensor

You interact with our systems on a daily basis, as such you know better then anyone else what is and what is not normal behavior. As a result you are one of the first that can determine if a system is compromised. In many ways you are a human sensor and can help detect and report intrusions. Here are some indications to look for that a system has been compromised.

- *Strange or unknown processes running on the system.*
- *Strange or unauthorized accounts have been added.*
- *Files larger then one gigabyte in size or files with odd permissions.*
- *Any new or unauthorized open ports or established network connections.*
- *Passwords are no longer working, even though you know they are correct.*
- *The system's browser is forcing you to websites you do not want to go to.*

If you see any of these indicators, please report it to our IT help desk or security team.

At times you may need to research new technologies or learn more to troubleshoot existing technologies. If this is the case, be very careful what information you share about our organization with others, such as on public maillists, with vendors or attendees at a conference. Do not share any sensitive or confidential information or provide attackers data they can use to harm our organization. Something as simple as IP addresses, host names or standard configuration options can provide attackers the information they need to exploit our networks.

When troubleshooting issues with your vendor support team, only share the absolute minimum information required. If configuration files need to be submitted to the vendor, the files should be first reviewed and all sensitive information should be removed, such as account names or password hashes. In addition, submit all information encrypted whenever possible.

Never download or install software from unauthorized or non-authoritative sites. Such software is usually tampered with or contains malware. Instead always download and install software from only trusted sites. In addition, do not install vendor-provided remote desktop control software or remote desktop viewing or diagnostic software without management approval.

As an administrator you are in a position where you can change the configuration of systems. Remember, depending on your department's rules you may have to get approval before making changes, especially any changes to baseline configurations. Always follow proper procedures, when in doubt simply ask.

Remember, as an IT Staff member you have tremendous access to our confidential information, systems and networks. As such you are also a primary target. By following these simple steps you help protect both yourself and our organization.