CYBER SECURITY
newsletter

HELP DESK

Problem

As part of our help desk team you are one of the most critical people in our organization. In many ways the help desk is the nerve center of our operations, it is where people go to ask questions and solve problems. You interact with a tremendous number of people and have access to a great deal of confidential information.

However, because of this access you are also a primary target for cyber criminals. You have been trained to help end users as efficiently as possible, and cyber criminals often abuse this goodwill. If they can exploit your computer or trick you into giving confidential information, cyber criminals can then cause a tremendous amount of damage.

For example, a cyber criminal may call the help desk and pretend to be a confused employee who has forgotten his username or password. Often the attacker will have a story to fool you, such as he needs to email an urgent report to one of the senior executives and is concerned about the consequences to both you and him if he fails to send that report. Since you have been trained to help end users, the attacker may trick you into resetting a password for him.

However, if you were to reset the password you would have just provided the cyber criminal access to our organization's confidential information. This is why it is so important that you first verify the identity of the person you are talking to using established procedures.

Help Desk

As a key member of the Help Desk, you have been trained to help others whom you do not know and whom you do not even see. Cyber attackers know this and may try to trick or fool you into giving out information. In this newsletter we explain several of their common attacks and how you can 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

Help Desk Attacks

Cyber criminals know you have been trained to help others, as such they may single you out. They will attempt to research our organization and identify what is the help desk email account or what is the help desk phone number, so they can contact you directly. Then they can do extensive research on the Internet, learning about specific employees through Facebook or LinkedIn. They can then use this combined information to contact the help desk, pretending to be an employee, vendor or contractor. This is why it is so important to always use proper authentication procedures.

If someone cannot properly identify themselves, or their request seems odd or suspicious, then simply tell them that policy dictates you cannot give them the access or information they are requesting. If the person persists, then escalate the call using proper procedures.

Solution

Once you have authenticated an end user, always follow all procedures to the letter, especially for actions like password resets, document restores, or providing additional information about our organization. Never give information or help people who are not properly authenticated or asking for more then they are authorized.

In addition to being a primary target for cyber criminals, you will often be the very first to know if other people in our organization have been hacked. You may even be able to identify trends that perhaps multiple people have been compromised. By identifying if our organization has been hacked, you can help our security team quickly respond and control the damage.

For example, let's say you receive a phone call from a Human Resources manager. She reports she cannot log into her computer, even though she entered her password correctly and now her account is locked due to failed login attempts. You follow the usual procedure, unlock her account and reset her password.

Several minutes later another end user rings the help desk. He changed his password the week before, but also seems to be unable to login. Again, you follow the usual procedure, unlock his account, and reset his password. You then continue to get an unusual amount of password reset requests throughout the morning. Something seems odd.

What you may not realize is that those end users did not forget their passwords. What happened instead is your organization got hit by a worm that has infected multiple computers and locked the end users out. The problem is no one has noticed the worm infection yet. By identifying odd trends such as this, and quickly reporting them to the security team or your supervisor, you can help us identify and stop attackers from infiltrating our organization.

Remember you have an important role in securing our organization, both in protecting the information you give out and identifying when our organization may be compromised.