GUARDSIGHT

https://www.guardsight.com

Cybersecurity Tips When Working From Home
Social Engineering

YOUR AWARENESS IS THE BEST DEFENSE

Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Examples include somebody pretending to be a help desk for your bank and asking for your login credentials or a contract job that seems too good to be true. A targeted campaign can be created against you with easily accessible information found on social media and other avenues to gain access to your sensitive work and personal data.

SIGNS YOU MAY BE A TARGET

- ➢ The situation or relationship is too good to be true. Actors look to exploit basic human survival needs.
- ➢ You are being overpraised for your skills or talents.
- ➢ The situation or relationship stresses its exclusivity.
- ➢ Lack of depth. Unable to verify the other party's background or claims is a red flag.
- ➢ Urgency to change communication channels.

For additional advice or to learn more contact us: info@guardsight.com

RECOMMENDATIONS

1	REVIEW POSTED INFORMATION	1. Review as much past and present information that has been posted to social media thoroughly. The weakest link in any computer network is the human link. 2. The information you share doesn't even have to be about your career for a threat actor to capitalize. Any information you make public (friends/family birthdays/anniversaries, pet's name, family member's name, interests, hobbies, etc.) can be harvested and meshed together to create extensive password lists to easily guess your password. 3. Vet any future posted information. Make sure the information you post is appropriate for the people you share it with.
2	REVIEW ACCOUNT SETTINGS	1. Periodically review all personal and professional online account settings. Indicators of compromise include things such as an unknown email forward address or unfamiliar answers to security questions. 2. Use multifactor authentication whenever possible. This added layer of security keeps malicious users locked out even if they have your password.
3	TRUST BUT VERIFY	1. Refrain from forming sensitive contacts online before verifying them some other way first. 2. Sensitive contacts include those where any large amount of money, proprietary/classified information, etc. is involved.
4	USE CONTEXT CLUES	1. Use as many context clues of your situation and environment as possible. 2. Not any one sign is an indicator of malicious intent on its own. Critical thinking is a great weapon.
5	REPORT SUSPICIOUS ACTIVITY	1. If you are asked to do anything illegal, report the activity to the proper authorities immediately. 2. It is ok to report suspicious activity as well. Police departments and local agencies have non emergency lines.