Communication

Essentially all roles in cybersecurity require a high level of both written and verbal communication. Every day you'll likely be replying to emails and messages, writing up reports or investigation notes, talking with members of your team, people from other teams, and even people from other organizations. In some roles, it is also likely that you will be presenting to groups of people, including peers, management, and non-technical audiences. Being able to talk to them at the appropriate level is important to maintain attention and get across the information you need to.

ONLINE COMMUNICATION

Regardless of whether you're emailing or messaging someone via an instant-messaging platform, you need to communicate efficiently and appropriately. You also need to be aware of any corporate policies that restrict how electronic communication is used, monitored, and stored within the organization. When emailing or using internal instant-messaging software, even if it's someone you're friends with, you should always act professionally as emails and chat history are stored and audited.

FACE-TO-FACE COMMUNICATION

Always remember when you're in a workplace, it is typically always a professional environment. It's great to have a laugh at work, but make sure it's not inappropriate and doesn't breach any workplace ethics or policies.

EXTERNAL PARTIES

When you're communicating with entities outside of your organization, it is important to remember that you are representing your company, so you must act professionally at all times. Never give out any information unless

you're sure you are permitted to disclose it to external parties. If you're not sure, ask a senior member of your team for clarification.

SOCIAL ENGINEERING

You're valuable. Not just because you're an awesome person, but because you know information about the company that outsiders don't. You know about the tools they use, internal IP addresses, team members, and lots more information that may seem pointless to you, but can be very valuable to attackers. If you publicly disclose that you work for an organization (Facebook status or employment section of your profile, LinkedIn post or employment history, etc) then you should prepare to receive social-engineering attacks at some point, where malicious actors try to get information out of you in harmless ways. Corporate policies can dictate what can and can't be shared online to reduce this threat, so make sure you read it if your organization has one. And please please PLEASE don't share photos of your work ID badge online! If you're traveling outside of the office, such as going to work or going home, out for lunch, or smoking outside, make sure your badge isn't visible (either in your pocket or if it's on a lanyard, inside your top). Malicious actors may attempt to view how ID badges look so they can design their own and use them to gain unauthorized access to the building.

Test out your security awareness skills using this in-browser game! https://www.isdecisions.com/user-security-awareness-game/

COMMUNICATION TIPS

K.I.S.S – "Keep It Simple Stupid" refers to using language that is appropriate for the audience, and that everything is clear and straightforward. If you're speaking to someone in a non-cyber department such as Human Resources, it's unlikely they'll understand what the suspicious connections coming from their work laptop are. It's often better to talk dumb to someone than use jargon and specialist vocabulary that they won't understand, which could give you a wrong answer and take up more time. This can apply for written communication such as emails and messages, and verbal communication.

If someone doesn't understand you, rephrase what you're saying. Don't blame them, and don't feel bad. Try to explain your message in a different way, giving them more information and time to understand what you're saying.

Body language matters. Obviously this only applies to face-to-face or video communication, but it's an important factor. It will keep your audience engaged, and helps to get across your message. Pay attention to the audience's body language, as it can help to identify whether they understand or if they're confused. Formal etiquette also applies in the workplace, and you should be actively showing you're engaged in communication by nodding, focusing on, and keeping eye contact with the speaker (plus it's just polite!).

Keep it professional. While the workplace can be a really social place, you always need to remain professional, after all, you're at work. There may also be company policies that you must abide by during working hours. Do not make racist, sexist, or otherwise derogatory remarks, and think about what you say to ensure it isn't inappropriate. Actions like this will be reported to the organization's Human Resources department, and it is likely they will take disciplinary action against any individuals involved.

If you're working from home, wear pants. There's nothing wrong with being comfortable, but remember you're still working, and need to remain professional! Especially if you're taking part in conference calls or meetings, don't be this guy, it's basic working-from-home etiquette, and it'll save you some embarrassment. (P.s – dressing smart while working from home could actually help maintain the professional mentality, helping you to focus on work instead of getting distracted).

Using RDP and SSH

How to Start Your Exam

Previous Topic

Next Topic

Privacy & Cookies Policy