Muninn

We See. We Act.

Cybersecurity Awareness Tips

Cybersecurity Tips

Version 2.0

GUEST LIST

HOW TO MANAGE VISITORS AT THE OFFICE

Many companies invest a lot to make their offices look representable and invite customers or partners to in-house meetings. But what about external parties who haven't undergone any vetting? The following guidelines can help you to ensure that data safety and cybersecurity are guaranteed:

- **Make sure unvetted visitors don’t wander around and keep an eye on them.**
- **Visitor pop-ins? Verify the identities of unexpected or unannounced visitors.**
- **Protect your Wi-Fi networks from unauthorized access.**
- **Be prepared and prioritize the vetting process for all visitors before their arrival.**
- **Notify your boss if something feels off.**

STRANGER DANGER

ENGAGING WITH UNFAMILIAR INDIVIDUALS

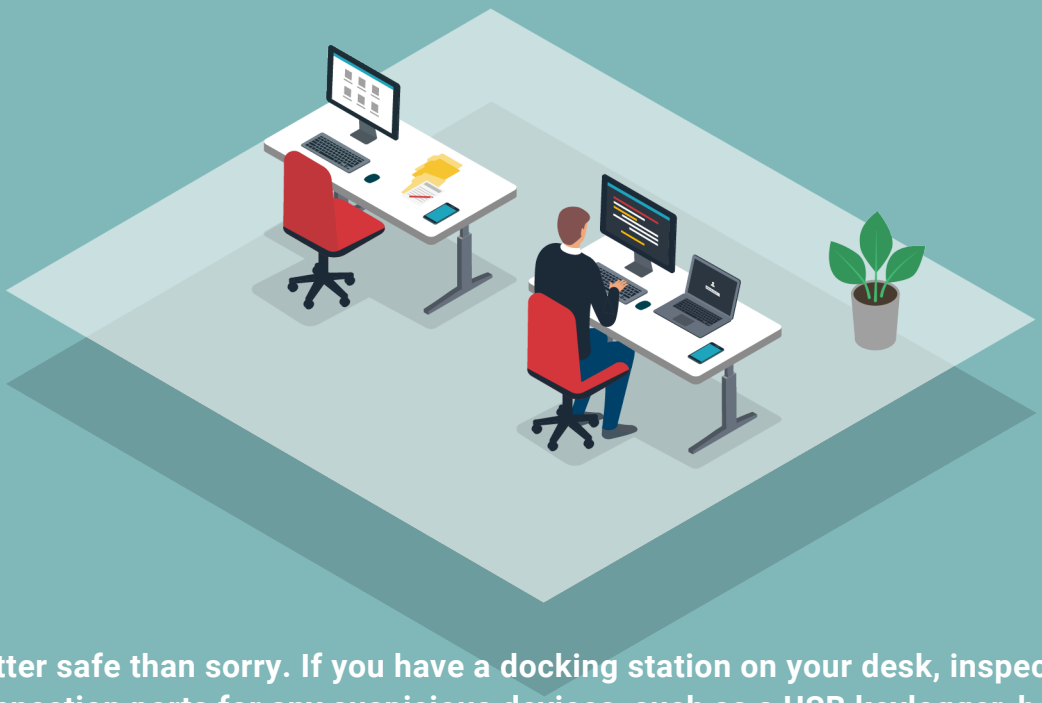
To many of us “social engineering” seems abstract and is done via social media and phishing emails. But it goes beyond a message on Instagram and happens offline as well. During physical interactions strangers may attempt to extract valuable information about your person, workplace or business.

- **Text message from an unknown person? Take the extra step of googling the phone number to verify their identity.**
- **You have heard this many times before, but it still happens: Do not open links shared by sources outside of your trusted circle.**
- **Don’t overshare. Instead of explicitly disclosing the name of your company, opt for mentioning the industry in which you work.**
- **If someone is too nosy about your work, redirect the conversation to a different topic.**
- **Avoid leaving your phone unattended on tables or at bars and keep that Bluetooth off around new crowds.**

TIDY & TIGHT

CLEAN DESK POLICY 101

Your desk is ground zero for data protection. A clean desk policy goes beyond an organized workstation and involves the daily removal of any sensitive business information such as USB's or printed documents from your workspace.



- **Better safe than sorry. If you have a docking station on your desk, inspect the connection ports for any suspicious devices, such as a USB keylogger, before connecting to your laptop.**
- **Daily declutter: Clear off sensitive documents and tech tidbits.**
- **Ensure that you are connected to the secure Wi-Fi network you typically use. Malicious actors may create deceptive duplicate networks to deceive you.**
- **Mystery USB? Inform the IT department or the Chief Information Security Officer (CISO) and report the incident.**
- **Quick coffee run? Lock your PC, every time.**

MULTIPURPOSE

USING YOUR DEVICES OUTSIDE OF THE OFFICE

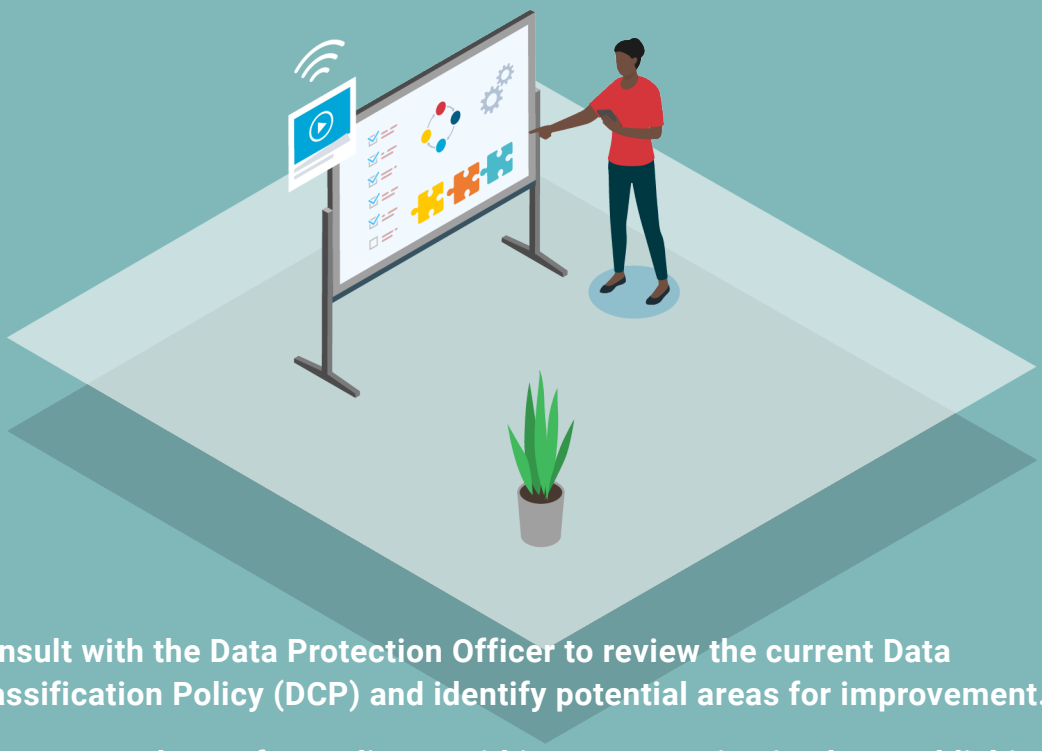
With the increasing trend of mobile work and employees frequently operating in public spaces, it is crucial to maintain vigilance regarding suspicious activities in your surroundings and the security of your computer and mobile devices.

- **Don’ discuss sensitive company information on your phone while in public.**
- **Disable the option to accept all incoming connections on Bluetooth and/or Airdrop.**
- **Always connect with a VPN (Virtual Private Network) for secure connections.**
- **Think twice before checking company emails in crowded spots.**
- **If you work on your laptop in public spaces like cafes, public transit, or parks, be mindful of “shoulder surfing” attempts. Consider investing in a privacy screen protector if you frequently work in public locations.**

BITS AND BYTES

LEVEL UP YOUR DATA GAME

It is essential to implement a data classification policy, because an effective data classification system can enhance operations, save costs, and moreover ensure compliance with regulatory requirements.



- **Consult with the Data Protection Officer to review the current Data Classification Policy (DCP) and identify potential areas for improvement.**
- **Promote a culture of compliance within your organization by establishing a clear strategy on how to handle data.**
- **Not all data is the same - focus your controls on safeguarding truly critical information. For instance, treat credit card data with higher security measures than a simple lunch menu.**
- **Regard confidential data as your company's most valuable assets and store it accordingly, implementing robust security measures.**
- **Knowledge is power. Develop training modules to educate your colleagues on data classification, providing guidance on the dos and don'ts**

STRICTLY CONFIDENTIAL

ELEVATE YOUR POWERPOINT GAME

Are you using PowerPoint or similar tools? Be mindful when sharing PowerPoint and other presentations. These applications are widely used to share information, both internally and externally. However, it is crucial to protect these presentations from unauthorized access, especially when they are sent via emails or file-sharing servers.

- **Think twice: Add less sensitive info on slides. Instead, verbally communicate the sensitive information during the presentation.**
- **Always set a password for the presentation when sending it via email and consider personally calling the recipient to share the password.**
- **Set a deadline: When sharing a large presentation file through a file server, ensure that you set an expiration date for the download to limit access.**
- **Consider adding a watermark to your presentation, including the date, name of the sender and recipient, and a confidentiality notice, when sharing it with others. Make it clear that this content is sensitive.**

AFTER WORK

LEAVING THE OFFICE

We have all experienced those hectic moments when we're in a rush to leave the office, whether it's to pick up our children from daycare or to make that cross fit class. Let's exit smart, not just fast.

- **Always remember to close and lock the windows near your desk before leaving.**
- **Scan your desk and leave no sensitive documents or drive behind unattended.**
- **Familiarize yourself with the security and alarm procedures in place at your office. This knowledge will help you avoid triggering false alarms in situations where you may arrive early or leave the office late.**
- **Are you leaving your work devices at the office? Make sure to lock them in a designated and safe storage, so they're ready for your next productive day.**

DON’T KEEP IT SIMPLE

POWER UP YOUR PASSWORDS

Your passwords are the frontline warriors. The most common vulnerability exploited by hackers is gaining unauthorized access to someone’s login credentials. In recent years, numerous companies have experienced data breaches, resulting in leaked user data, including login details and passwords on the dark web.

- **Get a password manager, as it makes your life safer and simpler.**
- **Don’t recycle passwords. Use unique passwords across different websites or platforms.**
- **Double lock access with multi-factor authentication (MFA) using app tokens or SMS on your phone.**
- **Stay away from post-it notes. Never write down usernames and passwords.**
- **Don’t spill your personal passwords with anyone, including your coworkers.**
- **Skip your pets name or ‘1985’ in passwords. Use random password generation feature in your password manager to create strong and unique passwords that you don’t have to remember.**

KEEP A COPY

DATA BACKUP BRILLIANCE

Data backups play a critical role in a company's ability to recover from incidents like ransomware attacks. Consequently, backing up company data has become an integral part of business continuity planning.

- **Know who is responsible for data backups within the company and take a deep dive into the specific implementation procedures.**
- **No mix and match. Keep your personal data separate from those official documents to maintain data integrity and protect sensitive information.**
- **Check law and other regulations: Make sure your back up's on the right side of GDPR and all other data laws.**
- **Doing the above? You are helping safeguard your company's crucial data.**

BE PREPARED

GAME PLAN FOR DATA BREACHES

Having a plan for any potential cyberincident is worth gold, but it's crucial that everyone is well-informed about what actions to take and what to avoid. To ensure preparedness, it is advisable to simulate a cyberincident and assess the company's adherence to the established plan.

- **Talk to the person responsible for the business continuity plan to understand the purpose and insights of the specific plan.**
- **Keep it secret and make the plan accessible to internal parties only.**
- **Frequent checks and updates. Evaluate whether the plan is still applicable in terms of the business systems, data included and technologies. Those might change over time.**
- **Feeling a bit rusty? Assess whether it is time to schedule another simulation to see if the current plan is still effective.**
- **Step up and stay up to date. Chaning your routines and mindset can bring your cybersecurity to a different level.**

www.muninn.ai

info@muninn.ai

+45 70 60 59 08