Digital Vigilance

Your Key to Robust Cybersecurity at Work

1. **Username & Password: Your First Line of Defense**
   Keep your digital gates locked! Safeguard your usernames and passwords as they are the first line of defense against cyber intrusion. Remember, password reuse is like using one key for all locks - a risk we cannot afford. Change them frequently for optimal security.

2. **Be Wary of Unsolicited IT Support**
   Received an unexpected call from someone claiming to assist with your IT systems? Exercise caution! Genuine IT support rarely operates this way. These unsolicited calls are often tactics employed by hackers to breach our secure network.

3. **Two-Factor Authentication:**
   Enhancing Security Upgrade your access security with Two-Factor Authentication. This adds an extra layer of protection to your login process, making it as hard to breach as Fort Knox!

4. **Safe Banking Practices**
   Our company policy is clear - we never request employees to transfer money to a new account. If you encounter such a request, it is likely a scam. Alert your bank and report the incident to our cybersecurity team immediately.

5. **Password Management: Keep it Fresh, Keep it Secret**
   Repeatedly using or recycling old passwords is an open invitation to hackers. Treat passwords like toothbrushes: change them often, don't share them, and definitely don't recycle!

6. **Email Protocol: Be Smart, Be Vigilant**
   Received an unexpected email with attachments or links? Halt! Verify first with the sender before proceeding. An ounce of prevention is worth a pound of cure.

7. **Software Downloads: Permission First**
   Downloading and installing software requires clearance from our IT department. Unauthorised downloads are akin to opening our secure network to external threats.

8. **"Free" Software:**
   Beware of Hidden Dangers Be wary of free software downloads; they may be carrying unwanted stowaways in the form of malware. Always stick to company-approved software.

9. **Cybersecurity is Our Shared Responsibility**
   Adhering to these guidelines will greatly fortify our cyber defense, deterring potential digital threats. Remember, in our digital workplace, your actions contribute significantly to our overall security. So let's work together to keep our systems safe and secure!

10. **Secure Financial Transfers**
    During any financial transaction, vigilance is key. If you encounter unrecognisable, new, or recently altered banking information, exercise caution. Contact the associated individual or business using their publicly listed number for a quick verification. Refrain from using numbers found within invoices or documents to avoid potential cyber security risks. This basic yet effective precaution could be a shield against fraudulent activities.

SECURITY IN DEPTH
www.securityindepth.com

Any Questions? Call on
1300 176 069
or support@securityindepth.com