Cybersecurity at Work Meeting Kit



WHAT'S AT STAKE

A single click on a bad link can cost your company millions. From ransomware to phishing scams, cyberattacks don't just target IT departments – they target people. That means you. If you handle email, log into systems, access client data, or even use Wi-Fi at work, you're part of the frontline defense. Cyber threats can shut down operations, leak confidential data, and ruin reputations. And they're not just a business risk – they can put your job, your identity, and your coworkers' safety at risk too. Staying cyber-safe isn't optional. It's part of your role, every single day.

WHAT'S THE DANGER

Cybersecurity threats don't always look like threats. They often look like harmless emails, friendly pop-ups, or routine login screens. But behind the scenes, they can open the door to serious damage – and it only takes one mistake.

Phishing and Email Scams – Disguised and Dangerous

Phishing emails are designed to trick you. They often look like they're from your boss, your bank, or a trusted vendor – but they contain links or attachments that, once clicked, allow hackers to steal information or install malware.

- Some phishing emails impersonate internal contacts and ask for urgent transfers or passwords
- Others include fake invoices or shipping notifications with malicious attachments

Weak Passwords and Reused Logins – An Easy Target

Using the same password across multiple systems, or choosing something like "123456" or your pet's name, makes it easy for hackers to break in. Once one system is compromised, they can often access others – especially if multi-factor authentication isn't enabled.

Ransomware and Malware – Lockdown Mode

Ransomware attacks can freeze your entire system — files, networks, even safety systems. You might see a screen demanding payment in cryptocurrency to get your data back. These attacks often start with just one infected file or link.

Unsecured Devices and Networks – The Silent Threat

Working remotely or using personal devices for company work? If those devices aren't secure or updated, they're an easy access point for cybercriminals.

- Even connecting to public Wi-Fi without a VPN can expose sensitive company data.
- Data Breaches – The Fallout is Real

HOW TO PROTECT YOURSELF

Cybersecurity doesn't need to be complicated — but it does require awareness. Most attacks don't start with some master hacker cracking a firewall — they start with someone clicking a bad link, reusing a password, or skipping an update. The good news? A few solid habits can make a big difference.

Think Before You Click

This is where most problems start — and where they can usually be stopped. Hackers love to send emails that look legit. Maybe it's "HR," or maybe it's "IT" telling you to "update your password now." They're counting on you to click first and ask questions later. Don't give them the satisfaction. Slow down. Look carefully. If something feels off — trust your gut. It's better to forward it to your IT team than fall for a fake.

Use Strong, Unique Passwords

This is one of the easiest steps you can take, and one of the most ignored. Think of your password as the lock on your front door — would you use the same key for your house, your car, and your office?

- Create passwords with a mix of letters, numbers, and special characters
- Don't use birthdays, pet names, or "123456" — those get cracked fast
- Use a password manager to help keep track (most workplaces offer or recommend one)
- Change your passwords regularly, and never share them — not even with coworkers

Keep Your Devices Updated

Yes, those software update pop-ups are annoying — but skipping them leaves the door wide open for cyber threats. Updates don't just give you new features; they patch security holes hackers know how to find. Whether it's your laptop, desktop, or mobile phone, keep it current. The longer you wait, the riskier it gets.

Secure Remote Work and Mobile Access

Working remotely or checking emails from your phone? That flexibility is great — until your data ends up in the wrong hands. Never connect to public Wi-Fi without a VPN, and always lock your screen when you walk away. If your company

gives you security tools, use them — they’re not optional. And if you use personal devices for work, make sure they’re protected too.

Be Smart with Company Data

Just like you wouldn’t leave sensitive paperwork sitting in the breakroom, don’t leave digital files unprotected either. Be thoughtful about how and where you access, send, and save information.

- Don’t save work files to personal USBs or drives
- Never send confidential documents to your personal email
- Use only approved apps or platforms to store and share files

FINAL WORD

Cybersecurity isn’t just the IT department’s problem — it’s everyone’s responsibility. One click, one reused password, or one skipped update can open the door to a data breach that affects your whole organization.