Cyber Training Guide

JUSTJUNK® Franchising Corp.
Updated: Mar. 2020

Cyber Training Guide

Table of Contents
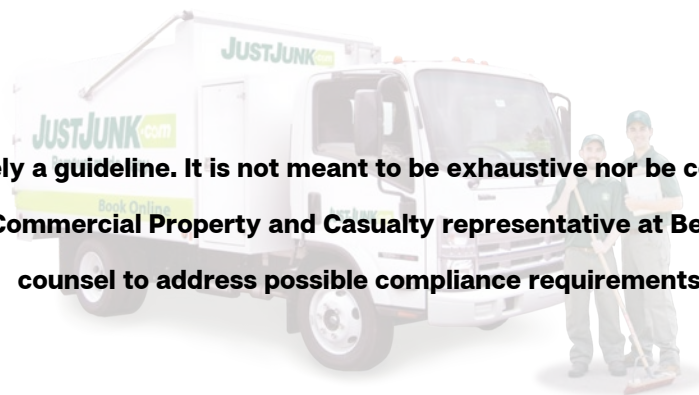
Cyber Training Guide

**Note: The material in this guide has been provided by
Benson Kearley IFG to JUSTJUNK® for reference.*

Introduction

The purpose of this document is to make you aware of cyber-security vulnerabilities and to give you the knowledge to protect yourself both at home and in the workplace. Although some of the topics covered in this training guide may not apply to you directly, it's important to read through them all to gain a background in cybersecurity procedures and the procedures that are specific to.

If you have any questions about cyber-security procedures—either at home or in the workplace—contact your manager or immediate supervisor.

Software Updates

What it means

When using devices, such as laptops, desktop computers, smartphones and tablets, you may see a small window pop up on the screen asking you to update your operating system (OS) or anti-virus protection. Although these windows can be irritating and are easy to ignore, they play a critical role in cyber security.

Device manufacturers and software developers use the always connected nature of today's world to constantly adapt to new cyber threats and push updates out to their users. Companies like Apple, Microsoft and Google can respond to a hole in their software and release a "patch" to fix it within a few days. Plus, there's an added bonus for you; these patches often include new features that will make your devices more capable.

Simple Security Tips

- Update the software on your computer and mobile devices whenever you're prompted.
- Check your programs and applications regularly to ensure you are using the most up-to-date version. If you aren't, be sure to download updates only from the official developer.
- If you've installed anti-virus software, be sure to run sweeps of your device regularly to check for malware and viruses

Making It Easy

Trying to figure out how to update your device and finding a time to do it can be harder than it sounds. However, many devices now support automatic updating. This means that when you aren't likely to be using your device, such as in the middle of the night, your device will automatically download any available software updates and restart.

OPERATING SYSTEM (OS):
An operating system is the software that runs on computers, smartphones, tablets and other devices. The OS is usually updated by the device's manufacturer or software developer to fix any existing holes in security, add new features and more. Common OSs include Apple's macOS and iOS, Google's Android and Chrome OS, and Microsoft's Windows.

Safe Internet Browsing

It's easy to assume that all websites are safe to browse, especially when you're using smartphones or other mobile devices. However, malicious sites can use tactics, such as internet cookies and phishing schemes, to gain access to your device or important personal and professional information.

Simple Security Tips

- When using a web browser, check the URL for a small lock icon to be sure that a site is secure.
- Additionally, a secure website will have an "s" in the "https://" that comes before the full URL.
- Never type personal or professional information, such as usernames, passwords, telephone numbers or addresses, into a pop-up window.
- If you ever suspect that a website isn't what it seems, close your browser immediately.

INTERNET COOKIE:
An internet cookie, also referred to as an HTTP cookie or simply a cookie, is a small amount of data sent by websites to your web browser, where it is then stored. Cookies enable your web browser to remember information, such as your username or browsing history, which can make it easier for you to browse online. However, other cookies can be used to track all of your browsing history or to keep track of your personal information. In the settings of your preferred web browser, there is usually an option to see and delete all of your saved cookies, which can help keep you safe as you browse online.

PHISHING SCHEME:
Phishing is a type of cyber attack in which a hacker poses as a trusted source online in order to acquire sensitive information. This is one of the most common and technologically simple scams there is, and it can put your personal and professional information at risk.

Additionally, hackers can use personal information to make the scheme seem more legitimate. If you post information in your emails or on social media accounts, hackers can use this personal information in order to trick you into giving up more information, or information about your friends and co-workers.

Secure Passwords

Making a new password can be one of the most frustrating—and important—things you do online. Every website and service seems to have different rules about length and complexity, and you have to add your password to an ever-growing list in your memory. However, knowing the details of what goes into creating a password can give you the insight you need to make a password that's both secure and easy to remember.

What Happens When You Make A Password

When you make a password, the service or website that you're signing up for usually encrypts the password before storing it on its servers. That way, even if a hacker were to gain access to your password through a cyber attack, he or she still won't have access to the text that makes up your password.

Hackers can use sophisticated programs to decrypt passwords, either by trying variations of common passwords or by "brute force," where a program will try every possible combination of letters, numbers and symbols in an effort to crack your password. That's why websites often require passwords to include uppercase letters, numbers and symbols. These special characters exponentially increase the number of possibilities that hackers will have to try in order to figure out your password.

Making Your Password

However, just because passwords should be long, doesn't mean that they have to be overly complex. As long as a password is long enough and includes a special character or two, it can thwart almost any attempt to crack it.

The next time you have to make a password, try typing in a favourite quote from a book, or a saying that's familiar to you. Turning a saying like "your guess is as good as mine" into "yourguessisasgoodasmine" actually makes for a strong, and in this case ironic, password. And, if you add a capital letter or special character as well, the password will only be that much stronger.

Simple Security Tips

- Make sure that your passwords include an uppercase letter, a number and a special character.
- Never keep your password written down somewhere, especially around the devices you use to access your online account.
- If you use a number of online accounts, consider using a password management tool. These websites and services require a single login, and will manage and save your passwords for you. However, be sure to research a service before you use it, as some have better reputations than others.

Installing Software

Software, such as apps and computer programs, make it easy to do work and access social media and other forms of entertainment. However, hackers can use malicious software to access your messages, contacts, emails and even your location based on satnav data.

Simple Security Tips

-
    When you download a piece of software, make sure to check how much access it has, and that it has been made by a reputable developer. Many apps and programs ask for more access to your computer or mobile device than is required.
- Always be sure to download an app from your device manufacturer's official store. If you download something from a website or a mobile link, it is much more likely to contain malicious code.

Social Media

Social media sites like Facebook, LinkedIn and Twitter allow us to easily connect with family and friends. However, they can also give hackers access to your personal information for phishing schemes. It's completely normal to check social media during the workday, but you should keep some best practices in mind. Please see the JUSTJUNK® Social Media Policy, which can be found in the JUSTJUNK® Online Resource Centre, for more information, or reach out to the Director of Public Relations.

Simple Security Tips

- Never talk about your work in social media posts without clearing it with a manager first. Even if you think something is innocent, it could give potential criminals an idea or insight into cyber attacks targeted against.
- Don't update social media when you're out of town. Although it can be tempting to post pictures and update your location for friends and family members, this will give everyone a clear picture of when you're out of the house and office. Then, anyone could use this information to steal from your home or office.
- Go into the settings of your social media accounts and check that your security settings are to your liking. Most social media sites allow you to block strangers and members of the public from viewing your information without your consent.

Record Keeping

When it comes to things like email and electronic bills, it can be easy to shrug off things like record-keeping. And, even though important things like receipts and account information are often stored as emails, you should take the time to think about organizing your digital information.

Additionally, you need to ensure that your data doesn't stay around longer than you want it to. Some OSs automatically save and backup your data into a cloud service to make sure it isn't accidentally deleted. If you want to delete something, you need to make sure it's also gone from the cloud and remote hard drives as well.

Simple Security Tips

- Whenever you make a large purchase or update important information online (e.g., licence plate renewal or new insurance coverage), take the time to print out this information and physically store it. You should also consider locking this information away to protect it from thieves.
- Create multiple email folders to store your messages. Folders could include topics like home, work, junk and finances.
- If you need to delete digital data, ensure that it has been deleted from all cloud services and remote hard drives.

THE CLOUD:

Simply put, the cloud refers to storage on a remote hard drive. Some OSs and other cloud storage services use a large amount of protected servers to store data, such as documents, pictures and videos, to ensure that data is safe and isn't accidentally deleted.

Additionally, the cloud can refer to accessing information or devices from a distance. This can include using a remote home security system, or something as simple as accessing a picture without downloading it to your device.

Because the cloud largely exists so your files aren't accidentally deleted, you need to be sure about what cloud services you use, and that you don't keep information on them for longer than you intend. Commonly used cloud service include Apple's iCloud, Google's Drive and Microsoft's OneDrive, as well as third-party services like Dropbox and Amazon's Drive.