Cyber Training

Device Security

Presented By:
Gallagher Risk Management - Tulsa

Gallagher

Gallagher

Table of Contents

Introduction: 3

Who Has Access: 4

Building Security: 6

Travel: 7

Portable Media: 8

Introduction

It's almost impossible to find a company that doesn't utilize technology and the internet in the course of its business. Those tools make information processing and storage much easier and more efficient than they have ever been before.

The devices that we use—laptops, smartphones, tablets and more—allow us to do more business in more places around the world. However, the more we use technology, the more attractive that technology becomes to cybercriminals. In all likelihood, you have access to at least one technological device that an enterprising cybercriminal could use to harm either you or your company.

It's not really possible to avoid those risks altogether. However, it is possible to reduce the chances of falling victim to a cyberattack—if you know what to look for and what to avoid.

This guide will cover the cyber risks posed by your devices. We'll cover a number of topics, including the following:

- Who has access to company device
- Device safety
- Building security
- Traveling
- Portable media

In this guide, we will cover some of the most common areas of cyberattacks. This training isn't intended to be exhaustive—we're only able to cover the basics in the time and space available. However, once you have a good grasp on the basics and develop a security mind-set, you'll be able to apply the same set of principles to a whole host of threats.

Who Has Access?

Company devices can contain all manner of sensitive information. Copyrighted materials, patented technologies or even private employee data may be stored on company devices.

Your company may have provided you with access to the following:

- A computer
- A laptop
- A mobile phone
- A tablet

A criminal could potentially exploit any of those devices to gain unauthorized access to your company's network or its data. That's why it's important to keep tabs on who might have access to your device. That could include any of the following:

- Family
- Friends
- Co-workers
- Guests
- Vendor

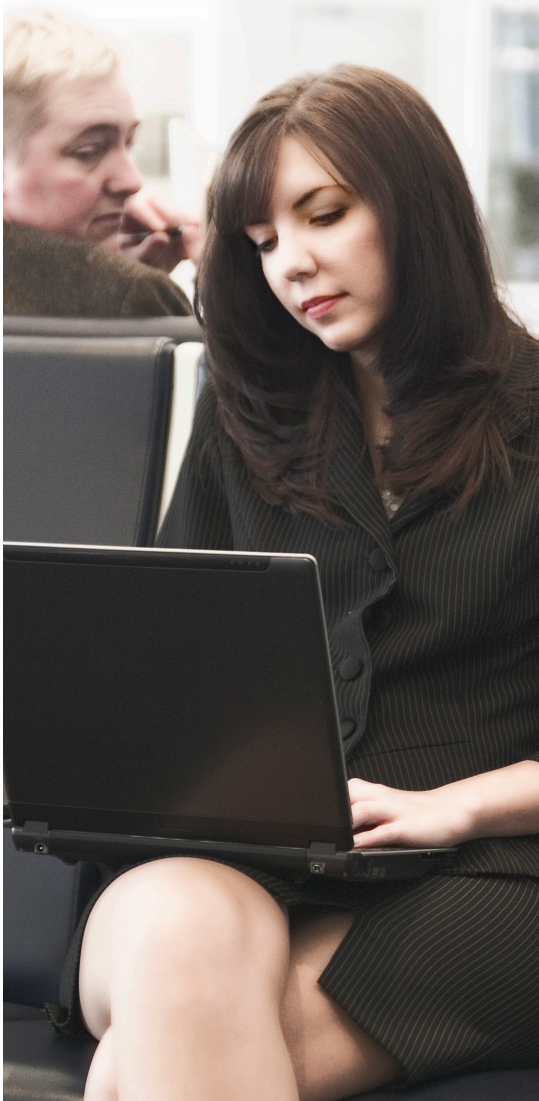
Who Has Access?

Device Security

Anyone—even someone you know well and trust—could potentially use your device as a point of access for a criminal attack. Sometimes, the people you allow to use your device might actually have criminal intentions. Even if they have the best intentions, a trusted friend or co-worker could accidentally allow a hacker remote access to your device.

Keeping your devices secure doesn't mean you have to become paranoid. It just means that you need to form some good habits and follow a few simple rules:

- When you walk away from your device, make sure it's protected by bringing up the device's lock screen.
- Make sure your device is set to automatically lock after a few minutes of inactivity, in case you forget to lock it.
- Never leave your device unattended in a public place.
- Only allow others to use your device with your expressed approval and supervision.
- If you suspect someone might have used your device without your permission, or you suspect someone has done something that could put the system in jeopardy, contact your manager and/or information technology (IT) services immediately



Building Security

Movies and television have created the image of the hacker as an individual who's sitting at a computer in a dark room, clicking on his or her keyboard. That image, however, conceals a troubling reality.

Often, hackers gain access to a system by physically breaching a company's security measures. After all, criminals are after the path of least resistance. Why write a complex computer program if the criminal can just walk up to your workstation and find your username and password written down on a notepad?

Typically, once someone has gained access to a building, he or she will be able to move around fairly freely. That's why it's important to follow these tips:

- Don't allow any unauthorized visitors into your workplace.
- If someone claims to be there to see someone, confirm with that person that he or she is expecting a guest. Make sure that the co-worker comes out to greet the guest and escorts him or her around while the guest is on-site.
- Make sure to close and lock offices, filing cabinets, lockers or anything else that could contain sensitive information.

Travel

Cyber threats can always strike, but the risk can be especially high when traveling for business. Often, business travelers will have to take extra precautions when traveling. Here are some important things to remember when traveling with devices from work.

Lock Your Devices

Lock screens ensure that unauthorized users can't access your devices. Make sure your devices are set to lock if they're inactive. That way, if you step away or accidentally leave a device somewhere, no one can use it.

Install Updates

The software you run on your computer—especially your antivirus software and your operating system—are constantly under attack from cybercriminals. That's why the people who design that software are constantly looking for vulnerabilities and designing solutions. Before you travel, make sure you've installed all available updates.

Portable Media

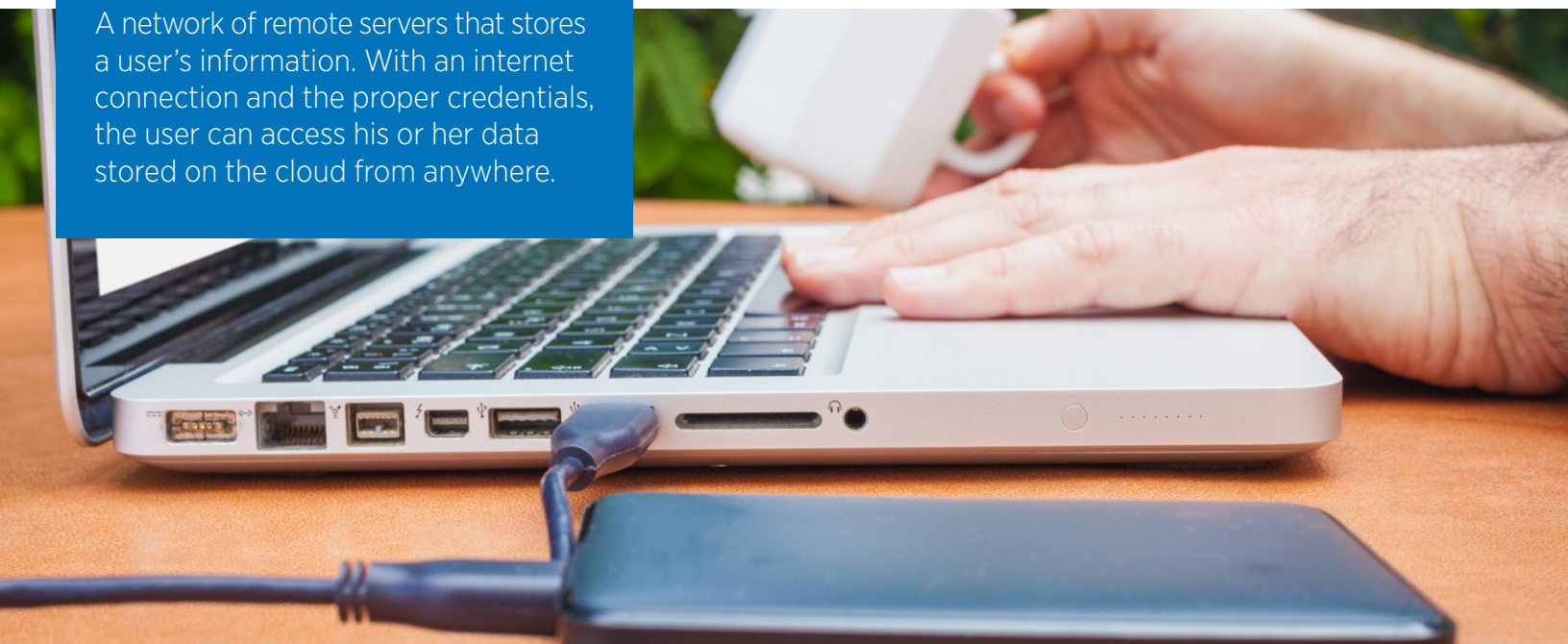
Many companies and individuals store files in hosted cloud drives. However, sometimes, you may find yourself transporting files on a USB flash drive, portable hard drive or other portable media device. When doing so, make sure to keep tabs on the device.

When you're using portable media devices, follow these safety tips:

- Password protect your files.
- Store important data on separate devices. That way, if one of your portable devices is lost or stolen, whoever finds it won't have all of your important information.
- Back up your data. Just as you need to make sure you're not giving away all of your important information if you lose a CD or flash drive, you need to make sure that, if you lose a portable media device, you're not losing your only copy.
- Remove devices properly. Damaged or corrupted data can be just as costly as lost or stolen data. Remember to use the proper commands to eject flash drives or SD cards before physically removing them.

The Cloud:

A network of remote servers that stores a user's information. With an internet connection and the proper credentials, the user can access his or her data stored on the cloud from anywhere.



Portable Media

Avoid Public Wi-Fi

Public Wi-Fi can make your life easier when you're traveling, which is something cybercriminals count on. In fact, they've been known to set up hot spots in public places like cafes, airports and hotels to try to get unsuspecting business travelers to connect. That's because, once you log on to a network, the person who set up the network or other users on the network might be able to access your device. If you're going to use a Wi-Fi network, make sure you can trust its source. Make sure the network that you access is encrypted. And, if you have to use an unencrypted public network, avoid going anywhere that will require you to enter your username and password.

Turn Off Auto-Connect For Wi-Fi and Bluetooth

Phones and tablets usually have an "auto-connect" feature that will search your surroundings for available Wi-Fi networks and connect to them automatically. Likewise, most phones and tablets are able to search for Bluetooth devices and connect automatically if you wish. For all of the reasons mentioned above, it's best to disable this feature on your phone while you're traveling. That way, you'll be able to determine which networks or devices you want to connect to and which you don't.