Contents

[1. Understanding the impact of cybercrime 1](#_Toc505960375)

[2. The real threats 2](#_Toc505960376)

[3. How your behavior can be exploited 3](#_Toc505960377)

[4. Personal workplace protection 6](#_Toc505960378)

[5. Getting the best out of passwords 7](#_Toc505960379)

[6. Safe and secure email use 9](#_Toc505960380)

[7. Virus and spyware protection 10](#_Toc505960381)

[8. Safe and secure web use 11](#_Toc505960382)

[9. Social engineering 12](#_Toc505960383)

[10. Security outside the workplace 14](#_Toc505960384)

[11. Intellectual property rights 16](#_Toc505960385)

[12. Privacy 18](#_Toc505960386)

# 1. Understanding the impact of cybercrime

You’ve probably heard about the rapid growth of cybercrimes like hacking, computer viruses, and identity theft, and the impact they have on businesses around the world. But are you aware of the direct impact that cybercrime can have your workplace, or how those attacks on the workplace could affect you personally?

Malicious software, or malware, is a term used to describe many closely related threats including computer viruses, Trojans, spyware, and bots, and is a constant threat to any workplace. Malware can be used to disrupt networks and communications, steal data, forward spam and any number of other malicious and costly tasks. It can also harm expensive computer systems and networks, which often have to be repaired, re-configured, or just simply replaced.

And with thousands of different types of malware in circulation it’s easy to see how just one can take advantage of a careless user.

Data like customer database are always a hot commodity, but financial records, design and development, strategic plans, business strategies and even general information on the way you do things in your workplace can also fetch a very high price. Even your personal payroll information can be valuable.

Lost productivity is one of the major sources of loss when a hacker or virus attacks, and email systems are one of the most common targets for attackers. Email is the best way to deliver viruses and the other Malware because the authors of this Malware rely on your predictable behavior – to open the infected emails and unleash the infection into our company. They know how much workplace like yours depend on email for everyday business.

Most organizations take a proactive approach to security, because it’s much less costly to prevent a security breach or incident than it is to recover from one. And even when there is a security breach, the better you get at security the shorter the incident will be, the less impact it will have, and the less it will ultimately cost your organization.

Cybercrime also has a major impact on customers. Most customers simply don’t feel comfortable exposing their confidential information to companies who are vulnerable to attack. And further damage can be caused to reputation if security or privacy is compromised by the careless or malicious behavior of seemingly trusted employee. The theft or compromise of design secrets, future business plans, and similar other data can all have a serious effect on competitiveness.

The hidden victims in the middle of this crime spree could be employee like you. No employee wants to be the sleeping sentry that lets in a catastrophic hacker or virus. Yet for many of these attackers you’re exactly the soft target they’re looking for.

And perhaps the greatest impact cybercrime can have on a company is the potential damage to brand and reputation. Brand and business reputation are an organizations most valuable assets, and any security breach or incident can potentially irreparably harm that reputation or brand in the eyes of customers.

# 2. The real threats

There are dozens of different types of potential threats behind this wave of cybercrime, but most fall into one of just four categories:

Hackers, which can include anything from opportunistic amateurs to professional data thieves.

Malicious software, or Malware, that includes computer viruses, spyware, bots, and other malicious code that can cause enormous harm and disruption to networks and business practices.

Spam or junk email that not only clogs networks and wastes your time, but usually contains some kind of fraudulent scheme.

And Insiders and Employees usually the people you least expect to harm your business or workplace but who often do so simply by mistake.

Some of these threats will fall into all the other categories. For example, professional data thieves are increasingly using viruses and spam as a way to enter company computer networks and steal information that could then be used in an identity theft. So it’s important that you understand these threats and their motives in order to recognize them before it’s too late.

Hackers are one of the biggest dangers to any workplace, because just like viruses, there are so many different types you have to defend against. Your workplace can be vulnerable to a number of different types of hackers, each with their own motives and agenda. For example, some hackers are simply interested in destroying data and systems or disrupting business processes. Data thieves, petty criminals and even organized gangs are constantly targeting any information that can be sold on the black market or maybe even offered back to the company for a ransom.

Hackers can find useful information in almost any company, such as:

Customer databases

Trade and design secrets

Payroll information

R&D programs

Financial data

And marketing plans and strategies

A growing type of hacking is focused on data espionage as local and foreign organizations try to steal or purchase information on their competitors.

There are also thousands of known types of computer viruses and spyware in circulation, and they are just as dangerous to the workplace as hackers. Viruses and spyware can harm your workplace in a number of ways including damaging computer systems, stealing or erasing data, and clogging networks. And a related threat called bots can install malicious code on your computer that will allow a hacker to take control of your computer and use it to relay spam, attack other computers, steal data and cause many other serious problems.

Spam and Junk emails are on the rise, and some experts believe that spam email accounts for more than 60% of all email received. Spam can also carry serious security risks like computer viruses and fraudulent schemes. In fact, most spam is fraudulent and is created to trick employees into unwittingly participating in some fraudulent schemes or virus attacks.

One of the biggest causes of loss of cybercrime is security breaches by seemingly trustworthy employees and people who can attack from inside the workplace, probably the last people you’d expect would want to harm their own workplace. But not all security breaches by employees are deliberate crimes. Often security is compromised because of either innocent mistakes made by employees, or by a failure to follow security guidelines and policies. But whether deliberate or accidental, security breaches created by employees from within the workplace are a constant risk which is why it’s so important for you to be aware of this risk and bolster your defenses from the inside and outside.

It’s important to understand that hackers, identity thieves, virus authors, spammers and disgruntled or dishonest employees are the main culprits behind cybercrime, and all of them depend on exploiting your behavior in some way. For example, as soon as you open a virus infected email, even when your instincts told you not to, you have just become part of the crime even if you had no prior knowledge. And ignoring your suspicions about a fellow employee just because you don’t want to be a tell-tale won’t stop the crime from happening. Security is everyone’s job!

# 3. How your behavior can be exploited

It’s often said that hackers, virus authors, identity thieves and other cybercriminals are “A” students of human behavior. And they spend much of their time studying the predictable behavior of employees like you as a way to find just one vulnerability they can exploit in an attack on your workplace. The purpose of their study is simple – to create attack strategies and scenarios that will take full advantage of your predictable behavior, and use you as an easy way around security defenses. Their ultimate goal is to turn you into an unwitting accomplice in their crimes against your own workplace. There are many kinds of behavior that hackers and other intruders find easy to exploit, and exploitable behavior can include:

Poor password habits, such as creating weak predictable passwords, or sharing your passwords with others.

Poor e-mail habits, such as opening obviously suspicious emails or sending confidential information by email to third parties outside the workplace without proper security.

Poor workplace security, like not logging off your computer when you’re not using it, or keeping a written password hidden somewhere around your desk.

Your willingness to be helpful, such as giving your password to a telephone caller just because the caller claims to be from your department.

Forgetting about security outside the office, such as not protecting a company laptop or not taking proper security precautions when telecommuting from home or from remote locations.

Ignoring security rules and policies in ways that allow intruders to bypass security.

And your reluctance to report your suspicions, whether it’s about security incident, the behavior of a co-worker, or unusual requests or activities.

Hackers, virus authors, identity thieves and other attackers often regard employees as sleeping sentries whose lack of vigilance makes it much easier to launch an attack. And they’re usually right. That’s because most employees only think about their role in security after an attack, such as a virus infection. Few employees think about security and cybercrime as they go about their everyday business, just as few employees think about the security implications before they open an email or share a password. Poor password habits are a major vulnerability. Your password is one of the most valuable prizes to any attacker, because it gives the attacker the opportunity to enter a network and spend as much time as needed to discover vulnerabilities.

Your Predictable Email Habits can create a major vulnerability, especially to computer viruses, identity theft schemes, and spam. Most of us regard email as a valuable and essential communications and productivity tool. But hackers and virus authors regard email as a weapon to deliver viruses and other malicious code, to steal passwords, to crash networks and computer systems, and to achieve maximum spread and impact. Email is a favorite target for attackers because it is such effective way to attack a single organization, or target thousands of organizations around the world. Email systems are also used for much targeted attacks, such as obtaining passwords, because email can be created to exploit the anticipated behavior and expectations of the recipient.

As employees you know the importance of being polite to customers, whether it’s on the phone, by email, or in person. And most people are naturally helpful in workplace, especially towards fellow employees and visitors. But just like email, hackers and virus authors don’t regard helpfulness as an essential part of the job, instead they view it as a weapon that can be turned on employees like you. Some hackers are confident enough to walk into a building, posing as an authorized employee or contractor, and looking for the first helpful employee that will fall for the ruse.

Poor workplace security can also lead to security vulnerabilities. For example, a fellow employee with less-than-honest intentions may be able to look over your shoulder as you enter password, only to use that password later to bypass security for any number of reasons. Intruders also know that employees will often keep passwords written down and hidden around their workplace; will forget to lock filing cabinets containing sensitive or confidential information; will forget to log off when they leave their computer for an extended time; and will often leave data discs lying around their desks. All of this behavior is well known to hackers and they’re always on the lookout for such an opportunity.

Your reluctance to report suspicious incidents can also create vulnerabilities. All your life you’ve probably been scolded not be a tell-tale, and our society has reinforced the message that reporting behavior or incidents by other people we know is somehow inappropriate. This is the kind of thinking that is not only exploited by hackers and virus authors, but by fellow employees who may be breaking security rules, behaving inappropriately, or even committing a crime, before your very eyes. In doing so, they are usually counting on your reluctance to report them, and you may even justify your inaction by arguing that security is not your job.

Forgetting about security when you’re outside the office is another potential risk, and while it’s understandable, it is never wise, simply because if you’re doing any work outside the office, whether while you’re travelling or telecommuting, intruders are always looking for that one moment when your guard is down. The most common way your behavior might be exploited outside the office is often the most obvious. The theft of a company laptop, for example, could be a very easy way for an intruder to steal information or find passwords. Failure to use required security measures on home computers could also be used by a hacker as a way to attack your workplace through a back door.

And finally, ignoring security rules and policies is not as unimportant as it might seem.

It can often seem tempting to ignore a security rule just once, or to bypass security or interfere with a security setting occasionally because it might be interfering with your job or the task at hand. But that’s exactly the kind of human response and behavior attackers expect, and they often launch their attacks to trick employees into ignoring security rules, just one time, so they can take advantage. And attackers only need one time or opportunity.

Information security policies are there for many good and important reasons:

They help to communicate security expectations so that employees understand clearly what they can and can’t do, and why. They help protect everyone at work from legal exposure that can often arise when a workplace does not have clear security guidelines that are properly enforced.

Hackers, virus authors, identity thieves and other attackers have found numerous ways to infiltrate computer networks and systems, and one of the most successful ways is the exploitation or predictable employee habits. In the words of one famous hacker “your employees are your security”

# 4. Personal workplace protection

Do you have a mental checklist of security do’s and don’ts that you refer to every day, when you arrive at work, and when you’re getting ready to leave at the end of the day? The answer is probably no, and the reason is because you probably don’t think that cybercrime and security are that important to need daily attention.

You should treat your workplace as your castle, and avoid the security mistakes some people might expect you to make.

Be careful about the web sites you visit, and be careful about any information you reveal on any web site.

Don’t download files from suspect web sites as they may hide unwelcome passengers like computer viruses or spyware.

Don’t share freeware or shareware in the office, and never make unauthorized or illegal copies of software or bring pirated software into the office.

If you perform your own personal backups of sensitive information, when you are working from the office or from home, back up often and store the backup media where it cannot easily be tampered with or stolen.

And pay equal attention to portable and thumb drives that can contain large amounts of sensitive data.

Make sure you back up regularly and according to your employers schedule or as required by company regulations. Performing quick backups of information that would be difficult or inconvenient to recreate, such as drafts of letters in progress, is also a good idea.

Don’t keep passwords or other security information around your desk.

Don’t leave sensitive or confidential files on your desk. Lock them in a drawer or data safe.

Shred sensitive or confidential documents when you no longer need them. Hackers will commonly even go through your garbage and company dumpsters looking for confidential information.

Make sure the security features on your computer are working and up-to-date and never disable or interfere with security settings.

Always challenge or report suspicious strangers, in the office, building, or parking lot.

If a stranger asks for directions to an office or computer room, offer to escort them.

If visitors do not display proper credentials, such as a visitor’s pass, contact your security department or escort them to the appropriate reception area.

You need to take personal responsibility for your own workspace and always make sure that you don’t inadvertently create opportunities for intruders. Take a look around you and if you see something that could create a risk, do something to solve it today.

# 5. Getting the best out of passwords

Your password is one of the most valuable prizes to any intruder, because it gives the intruder the opportunity to enter networks and spend as much time as needed to discover vulnerabilities or cause harm. And by using your password the intruder may be able to travel through company networks and computer systems unchallenged because the system thinks it's you.

Finding a weak password is not difficult as you might think. In one demonstration, a security expert using a very old personal computer, running a free popular password cracking program, was able to test 250,000 login and passwords combinations in just sixty seconds. Given that there are around 80,000 passwords in common use today, it would take even an inexperienced intruder less than twenty seconds to test all of the passwords in common use.

The following password tips can help make stronger passwords:

They should include CAPITAL or upper case letters.

They should include Small or lower case letters.

They should include Numbers.

And they should ideally include special characters or symbols, like the dollar or percentage symbol, or the colon or semi-colon character.

Ideally your password should have at least eight to twelve characters but always follow policy first. Every additional character you add to a password makes it infinitely more difficult for an intruder to guess or break your password.

By using a mixture of letters, numbers, and symbols you also make it much more difficult to find passwords, either by guessing them or by using easily available password cracking tools. And if you have trouble remembering long or complex passwords, we recommend that you use a pass phrase or password story to help your remember. For example, the simple phrase "I was born in August 1974!” could create a ten-character password, IwbiA1974!, that contains upper case letters, lower case letters, number and symbols. Just select the first letter or number in each word, and add a couple of capital letters. It's that easy.

There are a number of additional password rules that can help to prevent password vulnerabilities:

Never create passwords that are identical or similar to passwords that you used previously. That makes it easier for intruders who can use older or previously-used password to detect patterns and find newer passwords.

Avoid passwords that are based on a sequence of characters which are then partially changed based on the date or some other predictable factor (like a birthday)

Make sure you don't store your password on any computer or other electronic device where they might easily be discovered by intruders. This includes devices like laptops. PDA's, and even cell phones.

Never write down your passwords and store them in places intruders can find them. Places you should avoid keeping written passwords include desk drawers, on computer monitors, under mouse mats and keyboards, and anywhere around your desk or workplace.

If you think your password has been discovered by someone else, make sure that you change it immediately to a new and entirely different password.

Password should never be shared with or revealed to anyone else besides an authorized user.

Don't share your password with co-workers, family, or friends because even without knowing it, friends and family could inadvertently reveal your password to an intruder.

Never use words or names for passwords, especially family and pet names, rock star and movie star names, nicknames, or any words that can be found in a dictionary. Intruders expect such passwords and can easily overcome them.

Never give your password to a phone caller. Intruders often use techniques known as social engineering to try and trick users into revealing their passwords over the telephone. So if you're ever asked for password over the telephone, make sure you check with supervisor.

Never use home passwords at work. Your home security may not be as good as security in the workplace, and if a password you use at home is compromised, bringing it into the workplace could be bringing the intruder with it.

Be sure to change your password regularly, and every three or six months is ideal. Frequently changed passwords present additional challenges to intruders, and can help limit any damage if an intruder obtains your password.

And remember, if you need to send a password by e-mail or communicate it by any other electronic means, make sure you do so securely.

Passwords are like passports, and play a very important role in helping ensure that only authorized users have access to company resources. But in the wrong hands a valid password could give an unauthorized intruder unchallenged access to your most sensitive information. That's why you should never underestimate the power of a strong password, or the dangers of a weak one. So make sure you follow all password guidelines.

# 6. Safe and secure email use

We all recognize how important email is a business and a personal communications tool. But you should also understand that inappropriate or careless use of this valuable resource can not only create significant security and legal risks, it can also have a negative impact on overall business productivity and performance.

Email can be used to deliver and facilitate a wide variety of threats to your workplace including:

Computer viruses and spyware.

Spam and junk email.

Identity theft “phishing” schemes.

Virus hoaxes.

Scams and frauds.

Inappropriate workplace email such as diet promotions, “Get Rich Quick” schemes, and chain letters.

Offensive or illegal material such as pornography or hate material.

Network-clogging files like video clips, screensavers, and electronic greeting cards.

Email systems should generally be used only for business or job-related activities. Although most employees are usually allowed to use workplace email for incidental personal use, this personal use should be kept to an absolute minimum. That’s because excessive personal use of company resources can have an adverse impact on your workplace, reducing both company productivity as well as system and network availability.

In addition, certain messages and materials that are deemed inappropriate should not be sent or stored on workplace systems or networks.

This includes things like:

Messages for personal gain.

Solicitations.

Chain letters.

Lottery promotions and “Get rich quick schemes”.

And threatening, sexually inappropriate or harassing materials.

Email is such a common and comfortable communications medium for most people, it’s very easy to take it for granted and make mistakes. The best way we all have to avoid these security rules and guidelines, and understand that they’re there to protect all of us.

# 7. Virus and spyware protection

In addition to computer viruses, your workplace may also be at risk to spyware, key loggers, bots and other malicious code often designed to steal confidential information.

That’s why every employee needs to understand why and how computer viruses and spyware are such a threat, and what you need to do to prevent them. But viruses and spyware are not the only threats trying to make their way through email systems.

Spam can have an impact on networks and servers, taking up space and computing power that should be used for business purposes, and requiring your employer to invest unnecessarily in extra bandwidth and storage. And when the spam received in the workplace contains offensive content, it can create additional legal risks. Employees who forward spam such as chain letters, jokes, special offers, investment schemes, inappropriate and sexually offensive, and / or misleading e-mails to co-workers and others outside the workplace, risk creating liability issues for all involved. Spam is also being used by virus authors to increase the impact of their viruses, and by organized crime to launch identity theft scams. So it can be far more than simply irritating.

Virus and other malware authors exploit the predictable behavior of computer users, knowing that despite warnings users continue to open infected email attachments from people they don’t know or recognize. Many times the virus will have exploited the sender’s e-mail address book, tricking the recipient into assuming the e-mail is from a known source.

Education and vigilance are still your best defenses. Some recommended practices include the following:

Always follow workplace policies, rules, and best practices regarding e-mail use that are in general designed for your protection and also are intended to minimize wasted resources and maximizing efficiencies of your email system.

Never open e-mail attachments you weren’t expecting, or from people you don’t recognize. This is the most common way to spread viruses.

Don’t give in to temptation. Never open electronic entertainment files from suspicious sources, especially electronic jokes, greeting cards, screensavers, and music and movie files. These are also used to hide all kinds of malicious code.

Never forward these suspect files to co-workers or friends because if the file is infected you’re simply helping the virus creator to spread the damage to others.

If you receive a suspicious file, notify a supervisor or just delete it. But don’t take a chance by opening it.

Never interfere with or disable the anti-virus or other security settings on your computer, even just temporarily. This is behavior many virus authors expect and will readily exploit.

To help minimize the impact of spam, one of the best you can do is be very careful about who you give your email address to. Spammers are constantly sharing their lists, often harvested from web sites, so your email address on any public web site could end up on the lists of dozens if not hundreds of spammers.

Ask your friends and family to keep email they send to you at work to an absolute minimum. Remember that company policies usually specify that electronic systems and email are to be used for work purposes and allow for occasional and incidental personal use. If friends and family do send you an occasional email, make sure they don’t attach large files like vacation photographs or wedding video clips, as these can create log-jams in networks.

Never respond to spam, pass it on to others, or engage in any discussion with the spammer. Most spammers simply want you to reply to their email so they can confirm that your email address is real and they can sell it to other spammers. Today spam is mostly used to promote some kind of fraudulent scheme, so don’t fall for it. No matter how tempting.

# 8. Safe and secure web use

The Internet now contains millions of web sites and trillions of pages, and not all those pages are suitable or safe for access by employees during work hours. Inappropriate surfing during work hours can impact productivity, and create serious legal and security risks if employees share inappropriate material at work. And just visiting a web site could install malicious code on even a well-protected computer. So it’s important to make sure that you remain constantly aware of security when using the web at work and to keep personal use to a minimum and that you always follow security rules.

Remember that acceptable use of electronic resources usually allows for only incidental personal use of company computers, electronic assets, and web resources. Inappropriate web surfing, use of games, personal news groups, and other non-business activities should not use company resources.

Because of the importance of safe password practices when accessing the web, you should also avoid the temptation to save login and passwords on web sites that you use routinely as part of your work.

Viruses, spyware, and bots also remain a constant threat, and can hide in web sites and in information and files downloaded from the web. For that reason all attachments or files downloaded from the web or company sources on the Internet should first be screened with virus detection software prior to being used.

And similarly, you should not post sensitive, secret or confidential material, such as software, internal memos, or policies, on any publicly accessible Internet computer that supports anonymous FTP or similar publicity accessible services, unless you have prior approval and appropriate levels of security in place.

It’s important that sensitive information must never be sent over the Internet in an unsecured fashion. And for the same reasons passwords and other security information must never be sent over the Internet in readable form. This helps protect the information, your company, and you. It’s also never wise to publicity disclosure internal sensitive information via the Internet that may adversely affect the workplace or customers. Such information may include business prospects, products in research and under development, IT systems, HR issues and so on.

While it’s OK to make people aware of where you work, when you’re in mailing lists, chat sessions, social networking sites and other public places on the Internet, you should also clearly indicate that any personal opinions you express are your own and not necessarily those of your employer or company.

Whenever your workplace or company is mentioned with an Internet message or posting, it should adhere to the utmost standards of professionalism. You should always keep in mind that even several seemingly separate pieces of information can be pieced together by an outsider from a picture revealing confidential information which could then be used against the workplace.

In short, ideally you should never disclose more information than is required to get your job done professionally.

# 9. Social engineering

One of the most effective and dangerous techniques that hackers use to manipulate employees is called social engineering, and it’s vitally important that you learn how to recognize this serious threat. Social engineering uses social interaction as the primary means to trick or persuade you to disclose confidential information that can then be used to exploit your workplace.

The main goal of social engineering is to get you reveal your login and password, but it can also be used:

To obtain background information about things like facilities, people, and office practices for a later attack.

To learn “the lingo”, the internal jargon that will help a hacker sound like an insider in any future attacks.

To develop a relationship with an employee, build up trust and familiarity, and then exploit this trust.

To find a disgruntled employee that is an easier target for exploitation.

To gain unauthorized access to highly sensitive information such as customer files, including customer names, addresses, and credit card information; human resources and medical records; financial and sales records and much more.

Recognizing the tell-tale signs that an attacker is attempting to socially engineer you requires only one rule to remember: never give confidential information to someone you don’t know, especially never to a telephone caller. And in general anything that is marked confidential should not be disclosed to anyone outside or inside the workplace who has not been approved to view that information. Because most social engineering attacks are attempts to gain information that an attacker can’t easily get elsewhere, the mere fact that a stranger asks for the information should be a clear warning.

For example:

The hacker may pose as a computer support technician who needs to change your login name for the new computer system and needs your password to do so.

Someone in HR department who thinks your pay check has been paid twice to a person with your name, and needs your password to confirm you are the real you.

The senior executive who calls late in the evening complaining that he’s forgotten his password and needs yours so he can log on and access an important file for a crucial meeting in thirty minutes, and threatens to get you in trouble if you mess this up for the company.

These are just some of the warning signs that hacker may be trying to social engineer you:

Asking a password.

Asking for other “inside” information.

Excessive flattery or cajoling.

Threats: “If you don’t do it, you’ll get in trouble”.

Urgency: “I’m on my way to an important meeting”.

Reluctant to speak to a supervisor to resolve this issue.

Out of character. It’s just not the way things happen at your office.

Refuses to give a call back number.

Never ever give your password over the telephone or by email except when expressly authorized. If someone asks or threatens you for a password, offer to put them through to your supervisor or manager.

# 10. Security outside the workplace

Maybe you think that as soon as you leave your office or workplace, whether it’s on a business trip or just to head for home for the day, you don’t have to worry about security? After all, no hacker is going to know what your travel plans are and stalk across the city, right?

That’s the kind of thinking hackers anticipate, and while hackers are rarely stalkers they are always on the lookout for a careless employee away from the security of the office. Hackers and thieves are opportunistic and one of the best targets outside the office is the laptop. Hackers know that laptops can contain confidential files that are well protected on company servers but often have less protection when they’re on a laptop. Laptops also often contain important identification and authentication information that allows the user to access the company network from remote locations.

So make sure that the rules you learn about security in the office, you apply to work outside the office too.

Laptops and notebooks computers are not only target, and as PDAs, Smartphones and cellular phones become more powerful, hackers and data thieves are targeting them for any confidential data, passwords, and login information they carry.

Few of us expect to be the target of hackers and virus authors when we’re at home, away from work. But attacks on employees at home are increasing for one main reason: because employees usually drop their guard when they leave the office, and their predictable habits kick in with no security administrators watching them.

And remember, with modern storage technologies you can hold all of your company’s information in just the palm of your hand. Storage devices have changed, and a floppy drive, flash USB stick, SD Card and mini hard drive can fit in your pocket and yet contain millions of pages of important and sometimes critical information. So don’t get lazy or complacent think about securing these devices before a loss or theft occurs.

There are all sorts of vulnerabilities and habits that hackers can exploit which make employees a target at home.

Virtual private networks (VPNs) and other connections can be especially vulnerable if connection is left open on an “always on” connection like cable or DSL broadband, and can also be vulnerable if their security settings are interfered with.

Hackers and virus authors also know that many home users still don’t use properly configured firewalls and antivirus protection on home computers.

Some employees may be tempted to use a home computer, instead of company laptops, to work on at home. But they often forget that the home computer may have little, if any security installed.

Personal home computers used by kids are obvious targets for hackers. Hackers know that kids often have bad security habits, like downloading and sharing files from the internet, from music and videos to games and even homework. Any of these files can contain malicious code capable of stealing information from home computers, or hiding themselves on company laptops to sneak past security.

Kids will often share pirated software too, another popular delivery system for viruses.

Spyware and bots has become very popular as a hacking tool. Spyware and bots are pieces of code often hidden in free software or on infected web sites and which can be used by a hacker to steal information from the computer, send passwords across the Internet, and access company networks through the infected computer. In fact, you may only have to visit an infected web site to in turn have your computer infected by a bot.

Even petty thieves and burglars know the value of company laptops and data kept at home. Laptops are easy to steal and conceal, they can fetch a high price on the black market, and they can fetch an even better price if they contain valuable company information that can be sold to a trader in stolen information.

Your home may be your castle, but hackers and virus authors are not afraid to follow you there to take advantage of some very weak defenses. You wouldn’t leave your front door open when you are away so don’t leave your data open to others.

As an employee there are a number of steps you can take to protect yourself from cybercrime when you’re away from the office, and especially against the growing threat of laptop theft:

Always be vigilant, and aware that laptop thieves may be anywhere.

Where possible and practical carry your laptop in case other than a traditional laptop case. Use a laptop backpack for example.

Never leave your laptop, notebook, smartphone, cell phone, or PDA unattended, in a taxi, at a conference, in a hotel, a bathroom, bar, or airport.

If you’re in possession of portable and transportable computers or PDAs containing sensitive information where possible and practical avoid checking these computers into airline luggage systems.

If you carry confidential files on your laptop, make sure they’re protected. And always use encryption if required to.

If you’re accessing a network from off-site location such as hotel, airport, or your home, be extra vigilant. Only stay connected for as long as you need, make sure the appropriate access mechanism is in place, and don’t allow others to use your connection.

And when accessing web-based email be sure to log out and follow the instructions given on the screen to exit webmail securely when you are done.

And never leave your personal computer, PDA, or smartphone unattended with a modem turned on and communications enabled, and this is especially true if connected to company networks.

Don’t forget to protect your paper files as well. If you have to carry sensitive documents, keep them in a locked case and with you at all times. If you’re in a hotel, it’s best to lock them in the hotel safe when you’re not using them.

Protect your PDA and smartphone too. Don’t use them to store sensitive information like passwords, and make sure they’re password protected.

Don’t ignore security rules and common sense just because you’re away from the office. That’s when you may need them most.

That includes never downloading software from untrustworthy sources outside the company onto computers used to handle company data. This is very important because such software may contain viruses, worms, Trojan horses, and other malware that may damage information and systems. They could also introduce software incompatibilities and related technical problems.

And don’t forget about data protection either, whether it’s paper documents or computer media.

Make sure that you use a shredder to dispose of printed versions of sensitive information. All sensitive paper information and any information containing employee and customer personal information such as names and address, financial account numbers (like credit card numbers), etc. should ideally be shredded.

Similarly, any intermediate work products related to sensitive information, such as memo drafts, should also be shredded when no longer needed. Using a cross-cut shredder is considered a best practice.

By following these rules and remaining vigilant, you will not only help protect your workplace and customers but you can also help to protect yourself and your family from personal cybercrimes.

# 11. Intellectual property rights

Intellectual property is intangible product of the mind's work.

Intellectual property rights are the rights given to persons over the creations of their minds. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time.

WAYS TO PROTECT IP

Different forms of IP rights protect different aspects of the IP.

Copyright

Copyright deals with particular forms of creativity, concerned primarily with mass communication. A copyright is a form of protection provided to anyone who creates "original works of authorship." Essentially, a copyright protects literary, musical, dramatic, artistic and other qualifying creative works.

Computer programs are protected on the same basis as literary works.

Trademark

A trademark is any sign that individualizes the goods of a given enterprise and distinguishes them from the goods of its competitors. This definition comprises two aspects, which are sometimes referred to as the different functions of the trademark, but which are, however, interdependent and for all practical purposes should always be looked at together.

Patent

A patent is a document, issued, upon application, by a government office (or a regional office acting for several countries), which describes an invention and creates a legal situation in which the patented invention can normally only be exploited (manufactured, used, sold, imported) with the authorization of the owner of the patent. “Invention” means a solution to a specific problem in the field of technology. An invention may relate to a product or a process. The protection conferred by the patent is limited in time.

Trade Secret

A trade secret is a formula, practice, process, design, instrument, pattern, or compilation of information, which is not generally known, or reasonably ascertainable, by which a business can obtain an economic advantage over competitors or customers.

IP Rights in Ukraine

Ukrainian legislation provides that objects of intellectual property include without limitations:

• literature and artistic products;

• computer programs;

• data compilations (data bases);

• performances;

• phonograms, videograms, broadcastings;

• scientific discoveries;

• inventions, utility models, industrial designs;

• integrated circuits designs;

• rationalization proposals;

• plant breeds; animal breeds;

• commercial (firm) names, trademarks (signs for goods and services), geographical designations;

• commercial secrets, etc.

In Ukraine (like in the U.S., EU, and other countries) software, computer programs are protected by copyright. Protection of IPR in Ukraine is implemented through civil, administrative, criminal, customs, and anti-monopoly legislation.

Software and computer products in Ukraine are subject to copyright protection and certain IP rights violations may lead to criminal liability.

# 12. Privacy

Right to Privacy

The right to privacy refers to having control over yours personal information. It is the ability to limit who has this information, how this information is kept and what can be done with it.

In general, the right to privacy often means the right to personal autonomy, or the right to choose whether or not to engage in certain acts or have certain experiences.

The boundaries and content of what is considered private differ among cultures and individuals, but share common types.

Types of privacy

Privacy of the person encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private.

Privacy of behavior and action includes sensitive issues such as sexual preferences and habits, political activities and religious practices.

Privacy of communication aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail messages.

Privacy of data and image includes concerns about making sure that individuals’ data is not automatically available to other individuals and organizations and that people can “exercise a substantial degree of control over that data and its use”.

Privacy of thoughts and feelings means that people have a right not to share their thoughts or feelings or to have those thoughts or feeling revealed.

Privacy of location and space means that individuals have the right to move about in public or semi-public space without being identified, tracked or monitored.

Privacy of association is concerned with people’s right to associate with whomever they wish, without being monitored.

Limitations on the Right to Privacy

The limitation of right is set by many governments through requirements that interference must be made by a judicial authority or in a case when public safety or public order requires dissemination of the private information as prescribed by law.

Privacy in Ukraine

Information about personal and family life is confidential and may be disseminated only with the consent of a person, except the cases which are determined by law and only in the interests of national security, economic prosperity and human rights.

Information about personal and family life of individuals is any information about an individual, by which he/she can be identified or specifically identified, namely the information on: nationality, education, marital status, religious beliefs, health, financial status, address, date and place of birth, place of residence, on private property and non-property relations with other persons, including family members, on facts that take place in everyday life, intimate, social, professional, business spheres of life, excluding information on executing professional obligations by a person who is exercising state functions or functions of local authority bodies.