**UNIT-III**

**The Computer Passwords** are nothing but a series of character which is used to prevent from unauthorized access to computer system and networks. People use computer password which is also called as PWD for avoiding unwanted access to their personal data or information which has been stored or saved in computer memory [Hard Disk Drives].

The computer password may vary from 6 characters to 64 characters entirely depending upon the system where you are entering user secret key which in other term called as a password. People must use uppercase, lowercase digits, and special symbols to create a strong password which would be very hard to break.

Lets us talk about windows administrative passwords this are the PWD which secures unwanted access to the operating system hence avoid manipulations and stealing of your sensitive information from unwanted users. People generally save or store their personal information inside [computer system](https://www.chtips.com/computer-fundamentals/different-types-of-computer-system) which can be retrieved or cracked if it is not password protected.

Hence to avoid this kind of situation one must secure their computer system and network with password feature enabled. Now let’s talk about bios or CMOS password this computer utility program has all the features and almost all the system configuration information stored inside them and imagine if it goes to someone who has the access can change the sensitive information and eventually can damage your boot process and another setting which is important for proper [computer functionality](https://www.chtips.com/computer-fundamentals/functions-of-computer-system).

Therefore it is highly recommended to secure your bios configuration with a strong password. All the motherboard manufacturer provides us with the bios utility program you just need to press some special keys to enter CMOS or bios configuration. Some of the special keys are f1, f2, f10, Del and so on to know about your special key kindly refer your motherboard manual

**Different Types of Passwords?**

The Computer password is used in distinguishing and authenticating a user if the user has the correct secret key or password it allows them to access the computer system or network and likewise if the users don’t come with correct password it Denys the user to access the computer system or network. This is the privilege computer offers us which is very handy in terms of securing your personal and valuable information which is stored in computer memory.

**There are different types of computer password let us discuss a few of them.**

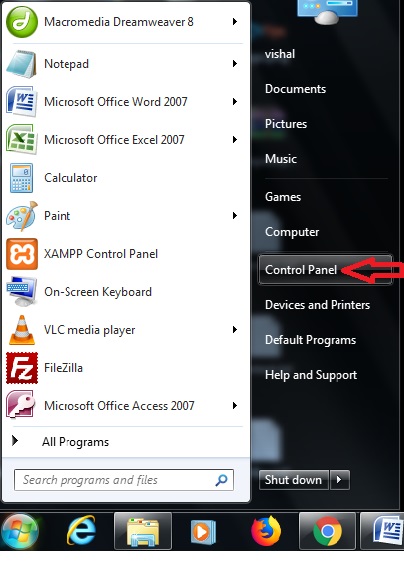
* CMOS | BIOS
* Administrative Password [Operating System PWD]
* Web Passwords
* Let us discuss them one by one. CMOS | BIOS Passwords:: These are the PWD which are generally stored in the CMOS battery which is called as complementary metal oxide semiconductor which is a small circular shaped cell allows to store passwords, date, time all the information stored in CMOS utility program.
* This is a lithium cell with 3.5-volt storage capacity installed inside a connector on the computer motherboard. If the CMOS battery is damaged it would not store any information given to it using bios programs. Users generally have to enter a key from keyboard to access the bios program which has all the features to change the system configuration suited to our need.

In BIOS utility program there are certain features where you can add a password to the computer system, change the boot order of computer, select boot devices and so on. You must create a CMOS or bios password to secure your sensitive information from unauthorized access and help the system to work to its full potential.

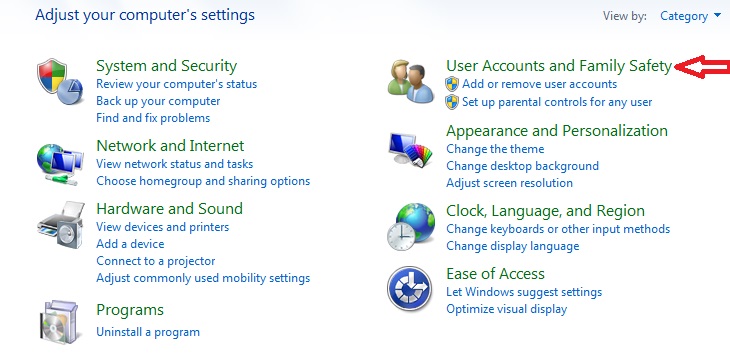
**Administrative Password [Operating System PWD]:** These types of the password are stored in computer memory that is computer hard disk drives to avoid access to unwanted users. This password generally used to prevent the operating system to load fully without one enters the correct secret key.If you don’t have the correct password or secret key you will be not allowed to access the computer system whether it be a host or in a computer network.

This PWD secures all your sensitive information stored in computer hard disk like credit card details, personal information which you would not share with anyone, personal photographs and so on.

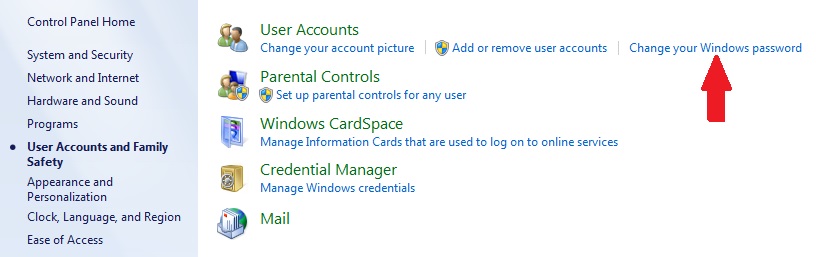
To create Administrative password follow the given steps.  
  
**Step 1:** Go to control panel by clicking on the start button.

Create Administrative Passwords

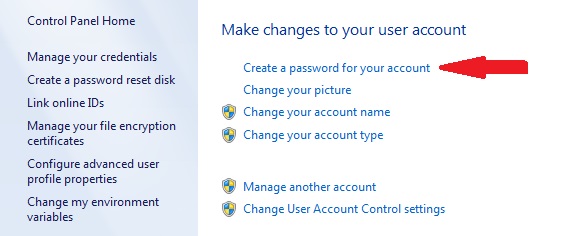
**Step 2:** Click on user accounts and family safety

Create Administrative Passwords

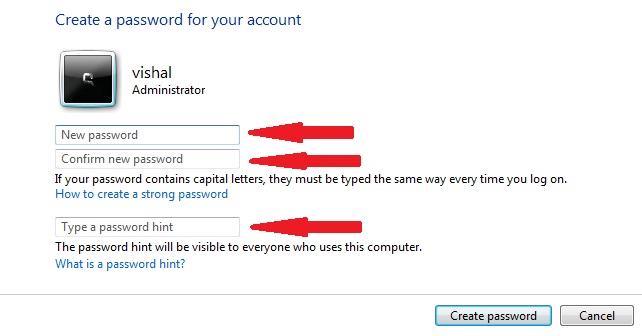
Step 3: click on change your windows password

Create Administrative Passwords

Step 4: click on create a password for your account

Create Administrative Passwords

Step 5: Enter your desired password and confirm the password…done.

**Create Administrative Passwords**

Web passwords:: Web password is used when working online for example before using any email program you first have to register in the website or application you have to provide them your credentials like name, last name desired username and password. These username and passwords act like your online identity.

Almost every application nowadays ask for registration as to know ones identify that you are a real person using their software or applications services. Some software developer has developed robotics programs which have spammed their services with fake accounts and illegal activities have been observed while using their services.

## Strong vs Weak passwords

**What are strong passwords?**

Strong passwords can be defined as PWD’s which are hard to break or guess.These passwords are created with the combinations of characters, digits and special symbols. For Example= Google++@32 is a strong password which is very difficult to guess and crack.

It is highly recommended that you must use space inside your password string that even makes it double to crack. You can also use uppercase and a lowercase letter for creating more advanced or strong passwords which would be highly difficult to crack by humans and computer programs. You must be extra careful while creating a PWD has some of the computer hackers with computer programs and tools will try to hack your passwords.

**What are weak Passwords?** **Weak passwords** are very easy to break and guess like some people use their names, birthdates, spouse name, children name or even their mobile numbers as PWD. For Example= John, 12-12-1990 and so on If you are using such passwords it is highly recommended that you change your passwords as soon as possible.

**Graphical Password Authentication**

With increasing technical advancements the world is becoming digital at a high pace and everything is happening online. From paying your bills to ticket bookings to paying the person sitting next to you, you prefer to pay online. Not only payments but all activities, be it, communication through e-mails and messaging apps, keeping your documents in a digital locker, etc happen online.

With everything turning online, the risk of cybercrimes and privacy breaches is also increasing. Passwords play a huge role in keeping your data safe online as well as offline platforms. Passwords are the default method of authentication to get access to our accounts. There are various types of authentication available for users to secure their accounts.

**Types of authentication**

* **Token-based authentication** includes key cards, bank cards, smart cards, etc.
* **Knowledge-based authentication** includes text-based authentication and picture-based authentication.
* **Biometric authentication** include fingerprints authentication, iris scan and facial recognition.

Considering the traditional username-password authentication, the alphanumeric passwords are either easy to guess or difficult to remember. Also, users generally keep the same passwords for all their accounts because it is difficult to remember a lot of them. Alternative authentication methods, such as biometrics, graphical passwords are used to overcome these problems associated with the traditional username-password authentication technique.

In a **graphical password authentication** system, the user has to select from images, in a specific order, presented to them in a graphical user interface (GUI). According to a study, the human brain has a greater capability of remembering what they see(pictures) rather than alphanumeric characters. Therefore, graphical passwords overcome the disadvantage of alphanumeric passwords. Graphical Password Authentication has **three major categories** based on the activity they use for authentication of the password:

* **Recognition based Authentication:**A user is given a set of images and he has to identify the image he selected during registration.  
  For example, Passfaces is a graphical password scheme based on recognizing human faces. During password creation, users are given a large set of images to select from. To log in, users have to identify the pre-selected image from the several images presented to him.
* **Recall based Authentication:** A user is asked to reproduce something that he created or selected at the registration stage. For example, in the Passpoint scheme, a user can click any point in an image to create the password and a tolerance around each pixel is calculated. During authentication, the user has to select the points within the tolerance in the correct sequence to login.
* **Cued Recall:**Cued Click Points (CCP) is an alternative to the PassPoints technique. In CCP, users click one point on each image rather than on five points on one image (unlike PassPoints). It offers cued-recall and instantly alerts the users if they make a mistake while entering their latest click-point.

**Advantages:**

* It is user-friendly.
* It provides higher security than other traditional password schemes.
* Dictionary attacks are infeasible.
* CCP makes attacks based on hotspot analysis more challenging.

**Disadvantages:**

* Registration and login take too long.
* It requires more storage space because of images.
* Shoulder surfing(Watching over people’s shoulders as they process information).

**Types of Password Attack**

Stolen, weak and reused passwords are the leading cause of hacking-related data breaches and a tried-and-true way of gaining access to your IT resources. And with billions of credentials available on the dark web, cybercriminals don’t have to go to great lengths to find compromised passwords. To get the best return on investment, hackers are looking for easy access—and improving your password security puts up more barriers for them to overcome.

There are different password attacks and ways to mitigate your risk, all following best practices for security:

## Brute-Force Attack

A brute-force attack is a type of password attack where hackers make numerous hit-or-miss attempts to gain access. It is a simple attack and often involves automated methods, such as software, for trying multiple letter-number variations.

Employing an extensive number of possibilities takes a long time, so attackers must look for efficiencies. To generate a list of potential combinations, they often start with easy choices, such as common or short passwords. If they know the password requirements for a specific provider (such as the minimum number of characters accepted), the attackers will apply those criteria as well.

## Keylogger Attack

A keylogger is spyware that records a user’s activity by logging keyboard strokes. Cybercriminals use keyloggers for stealing a variety of sensitive data, from passwords to credit card numbers. In a password attack, the keylogger records not only the user name and password but also the website or app where those credentials are used, along with other sensitive information.

Keyloggers can be either hardware or software. Since planting hardware on a device takes a lot of extra work, the threat actors are more likely to install malware on a computer or device by luring a user to click on a malicious link or attachment. Some keyloggers also come bundled with software (like “free” apps) that users download from third-party sites.

## Dictionary Attack

A type of brute-force password attack, a dictionary attack is based on a list of commonly used words and phrases, as well as often-used passwords. To avoid having to crack a long list of possible passwords, attackers narrow down the list to what’s known as dictionary words.

Those words are not limited to actual words in the dictionary. They could also include popular names of pets, movie characters and people. Hackers will also throw in variations by appending letters with numbers and special characters (e.g., substituting the letter O with number 0).

## Credential Stuffing

Credential stuffing is similar to brute-force in that attackers use trial-and-error to gain access. However, instead of guessing passwords, they use stolen credentials. Credential stuffing works off the assumption that many people reuse their passwords for multiple accounts across various platforms.

Over the years, numerous breaches of websites and cloud-based services have resulted in a massive number of [compromised credentials](https://www.sailpoint.com/identity-library/how-compromised-credentials-lead-to-data-breaches/). Just one single major-provider breach can yield millions of victim accounts, which cybercriminals then sell, lease or give away on the dark web.

Attackers use credential stuffing to verify which stolen passwords are still valid or work on other platforms. As with brute-force attacks, automated tools make these password attacks incredibly successful.

## Man-in-the-Middle

A man-in-the-middle scenario involves three parties: the user, the attacker and the third party with whom that the person is trying to communicate. In a password attack, cybercriminals typically impersonate the legitimate third party, often through a phishing email.

The email looks authentic and may spoof the third-party’s email address to throw off even savvier users. The attackers try to convince the recipient to click on a link that goes to a fake but authentic-looking website, then harvest the credentials when the user logs in.

## Traffic Interception

Traffic interception, a variation on the man-in-the-middle attack, involves the threat actors eavesdropping on network traffic to monitor and capture data. A common way of doing that is through unsecured Wi-Fi connections or connections that don’t use encryption, such as HTTP.

Even SSL traffic is vulnerable. For example, a hacker can use a man-in-the-middle attack in what’s called SSL hijacking. SSL hijacking is when someone tries to connect to a secure website, and the attacker creates a bridge of sorts between the user and the intended destination and intercepts any information passing between the two, such as passwords.

## Phishing

Phishing is a versatile approach. Cybercriminals use different phishing and social-engineering tactics, from phishing emails for man-in-the-middle attacks (as described earlier) to a combination of spear-phishing and vishing (a multi-step password attack that includes a voice call and a link to a malicious site that harvests credentials). The latter has been used in attacks targeting employees’ VPN credentials.

Phishing attacks typically create urgency for the user. That’s why the emails often claim a bogus account charge, service expiration, an IT or HR issue or a similar matter more likely to get the person’s attention.

## Password Spraying

Another form of a brute-force attack, password spraying involves trying a large number of common passwords on a small number of user accounts, or even on just one account.

Attackers go to great lengths to avoid detection during password spraying. Usually, they’ll do some reconnaissance first to limit the number of login attempts to prevent account lockup.

**How to Prevents Attacks**

The best way to prevent password attacks is to [adopt best practices for password hygiene and  management](https://www.sailpoint.com/identity-library/password-management-best-practices/). Easy-to-hack environments that have a weak security posture are much more appealing to opportunistic cybercriminals. Boosting password security significantly improves your ability to avoid a data breach. Password best practices include:

* Requiring long, complex passwords that are unique for each website or account
* Implementing [multi-factor authentication](https://www.sailpoint.com/identity-library/what-is-multi-factor-authentication/) whenever possible
* Adopting a password manager to simplify password management and to ensure secure storage

Your IT team should also limit access to privileged accounts and add additional security layers for those accounts. Of course, educating all your employees and other stakeholders about password security is also a proven means of prevention. With security breaches becoming the new norm, organizations and  their employees  can play a key role in maintaining their organization’s security posture.

## Password Management Solutions

Attacks are becoming more sophisticated as hackers adopt more advanced tools and automation. Implementing a robust password management program is not only a security best practice, but it also simplifies password management for IT administrators and employees—making jobs easier while reducing risk to your organization. Find the right solution for your current and future security needs with [SailPoint](https://www.sailpoint.com/demo/).

# Staying safe in a digital world

Whether you prefer a personal computer, carry a tablet or use a smartphone, connecting with the world has never been easier.

There's a darker side to our digital world, where threats to the privacy of your personal information lurk.

Phishing is one of the top 5 scams according to the Better Business Bureau. [CPA Canada](https://www.cpacanada.ca/en/news/canada/2018-08-14-five-scams-that-took-the-most-money-out-of-canadian-pockets-last-year) found that Canadians lost over $20 million dollars due to wire fraud and spear phishing in the previous year.

Not enough of us are tapped into how quickly cybercrime is evolving. Hackers creating mischievous computer viruses that wreak havoc is "old news". Now, the stakes are much higher as hackers focus on stealing your private information, your identity and your assets. According to the [2018 Norton LifeLock Cyber Safety Insights Report](https://now.symassets.com/content/dam/norton/campaign/NortonReport/2019/2018_Norton_LifeLock_Cyber_Safety_Insights_Report_Global_Media_Deck.pdf), more than a billion consumers have fallen victim to cybercrime, 800 million in the last year. Further, 117 million adults of all ages were impacted by identity theft in 2018 – 1.5 million in Canada. The most eye-opening: more than half of victims don’t realize that children are a target.

## Cybercrime: email and connected devices

Consumers are more attuned to safeguarding their personal computers from established risks. Consumers are taking steps to protect themselves, through keeping passwords private, not opening suspicious files, and limiting information shared on social channels. But email and connected home devices; where the public is less aware of the dangers – are also avenues for fraud.

Norton's research noted that 30% of consumers on a global scale are not aware that their smart devices can be hacked (including smart homes, TVs, door locks, and baby monitors). 1 in 4 consumers don’t know that unauthorized access to an email account may lead to access to all linked devices.

It is important to highlight the risks of cybercrime in an effort to prevent any further losses. Here are some of the most dangerous privacy threats to watch out for.

## Email Phishing

Phishing is when Internet scammers use email lures to “fish” for passwords and financial data from the sea of online users. Phishing attacks use “spoofed” (look-alike) email messages and fraudulent websites designed to trick recipients into divulging personal, business and sensitive information such as credit card numbers, account usernames and passwords or social insurance numbers. Under the guise of a reputable brand like a financial institution, credit card company or government agency, thieves will approach you with a bogus appeal to lure you into responding.

This might be a request to update your account, confirm billing information or enter a contest. That request often includes a time element such as a threat to cancel or close your account if you don't respond quickly.

The malicious email will direct you to click on a link connected to a web address that's standing in for a legitimate website. Once there, you'll be asked to provide personal or financial information like credit card details, social insurance numbers or banking passwords.

Phishing scams often target the financial and payment services sectors.

## SMS phishing

SMiShing, short for "SMS phishing", is similar to phishing. But it is the practice of using text messages sent to a mobile device in an attempt to get you to release personal information or click on a fraudulent link. Many people are unaware of this type of scam.

A SMiShing attack usually has a call to action for the intended victim that requires an “immediate response”.

BlueShore Financial has implemented a number of safety measures to combat scams including [security alerts](https://www.blueshorefinancial.com/WaysToBank/Online/Alerts/). One of which advises clients if an account has been locked due to three unsuccessful login attempts.

If you have any suspicions or concerns at any time, it's best to contact your financial institution directly.

## Voice phishing

Vishing or "voice phishing" works phone contact into the act. A visher calls and speaks directly to you or leave's a voice message to try to get you to call them back. Either in person or through an automated system, they then attempt to get you to release personal information.

## Angler phishing

Online customer service through social media channels like Face book and Instagram are vulnerable to fraud. “Angler phishing” is when requests for support or information to a legitimate company are monitored by scammers and then “answered” by the scammer asking for personal information or luring the victim to fraudulent websites.  
  
You can check that their “handle” matches other responses, but remember, a legitimate company will never ask you for personal details on a public network. If you’re unsure, call the company directly using a phone number you know is accurate.

## Spyware and ransomware

Spyware is a type of malicious software or "malware" that, once installed on your computer, allows criminals to monitor your behavior and gather valuable data. Spyware isn't intended to crash your system or wipe its memory like the computer viruses of the past. Instead, it works quietly in the background tracking your keystrokes, searching your hard drive and sniffing out your personal details to send to unknown parties.

Ransom ware on the other hand, is software designed to block access to a computer system until a sum of money has been paid. While often targeted to company networks, individuals have also been caught.

## Fake Hotspots

Public WiFi access is convenient, but not secure. Many people use free or unsecured Wi-Fi networks in airports, coffee shops and other public places. The perils of open Wi-Fi begin when you log on to a network that appears valid.

That free network may be nothing more than a gateway to track your activities, gather passwords you enter or view your sensitive information. Criminals will sometimes use a different tactic, setting up copycat hotspots with the same name as a legitimate network hoping to fool you into thinking you're connecting to the real thing.

## Smart use of your Smartphone

We live in a wireless world where technology helps bring many things, including banking, into the palm of your hand. But with this flexibility comes the need for attention to safety and a clear understanding of where your private information may be vulnerable.

Bluetooth technology provides a way to exchange information between wireless devices such as mobile phones, laptops, computers, printers, and digital cameras across a low-cost, globally available, short-range radio frequency band. It provides nearly ubiquitous connectivity, but it also can open the door to data theft.

When Bluetooth is enabled, it creates an open network to your mobile device. For sensitive information like mobile banking, we recommend you disable Bluetooth until your transactions are complete.

And use built-in Smartphone security features to their best advantage. Password protect your device. Use biometric authentication. Ensure you have the auto lock set to the shortest time possible. That way if you lose your phone (or it's stolen), you'll be protected.

## How you can protect yourself

Despite the sophisticated methods fraudsters are devising to invade your privacy, there are steps you can take to protect yourself.

#### 1.  Remember the essentials

A few basic steps will go a long way to protecting your personal information.

* Keep the operating systems on your devices current with the latest updates and patches
* Install security software that can detect viruses, spyware and other malware and provide a firewall to protect your data
* Use email spam filters
* New malware is appearing constantly so ensure your protective tools are set to update automatically
* Never send out confidential information (account numbers, passwords, etc) via email

#### 2.  Understand how reputable businesses act

It's easier to spot potentially dangerous communication if you know how trustworthy organizations behave. As an example, BlueShore Financial will never send you an unsolicited email asking you for your password, account numbers, confidential information, or urge you to restore your account access in this manner.

Here are some ways to spot a phishing email:

* Spelling errors or other anomalies in the sender’s email address and the URL (web site address)
* Requests for personal or sensitive information (username, passwords, social insurance numbers, banking information, etc.)
* Pressure for urgent action or response; the fraudsters are appealing to the human inclination to click embedded links or open questionable attachments
* Scare tactics and threats; ironically, a frequent ploy is to claim “your security has been compromised”.

Also remember, before entering sensitive data through the website of any company you deal with, make sure you first see the "https:" prefix or a padlock in your browser's address bar.

#### 3.  Verify, verify…and verify

Learning to be a skeptic can keep you safer online. Don't click on a link or call a phone number that comes with an uninvited email, pop-up or phone message without first verifying it's valid. Avoid opening attachments, links, or installing software from an unknown source.

When you're mobile, know what you're connecting to. Only download apps directly from a service provider's website or an authorized source (e.g. Apple App Store). If you must use a public Wi-Fi network, check with a representative of the place you're visiting to make sure it's a genuine connection.

Using the privacy settings on your mobile device, including the password or passphrase feature, will help protect your connection and keep your data secure should your device be lost or stolen.

#### 4.  Don't overlook old-school risks

It's no surprise that security in the Smartphone age concentrates on the digital channel. However that doesn't mean yesterday's threats has disappeared.

Be vigilant to identity theft and breaches of your privacy when you're offline as well.

* Don't write down PINs or keep them in your wallet
* Remember to sign your credit and debit cards as soon as you receive them
* Monitor your accounts and statements for unusual activity and shred confidential documents you no longer need
* It's wise to get in the habit of reviewing your credit report at least once a year

#### 5. Use complex passwords and change them regularly

Norton stresses that using complex passwords and changing them regularly is still one of the best ways to protect your privacy online.

When creating passwords, longer is better.

* Go with one that's at least eight characters in length
* Use a mix of upper and lower case letters, numbers and special characters
* Avoid choosing real words, numbers in sequence or personal information that can be easily obtained like your birthdates, names of family members or phone numbers
* Set a reminder to change your password every six months

#### 6. Take steps to protect you home network, connected devices and Smartphone

* Use two-factor authentification on home computers, email accounts and smartphones where both a password and a second authentification step are required
* Install anti-virus software on both your computer and Smartphone
* Ensure your home network is password protected by a password that you created, not the default password that comes with your router
* Password protect all your connected devices with different passwords
* Keep your personal computer on one network, and your connected devices on a second network - multiple networks can be set-up with many routers
* Never click on links in emails

Technology will continue to open doors to greater convenience in your financial life and beyond. That technology can be used more safely if you understand the risks and take the right steps to secure your privacy.