ASSIGNMENT 4

1) Web Browser Extensions: How risky are extensions & how can you choose safe ones?

Web browsers play an integral role in the way we interact with the internet. They're the gateway to the vast online universe, allowing us to shop, learn, communicate, entertain ourselves, and much more.

A web browser is a software that enables users to access and view content on the World Wide Web. Its primary function is to locate and retrieve web pages, images, videos, documents, and other files from servers and display them on the user's device.
For instance, imagine you want to visit a website. Here's where the browser comes in. When you type the website's URL into the browser's address bar and hit Enter, your browser sends a request to the server where the website's files are stored. This communication happens over protocols such as HTTPS (Hypertext Transfer Protocol Secure) or HTTP (Hypertext Transfer Protocol).
On receiving your request, the server sends back the website's files. These files are often written in languages like HTML, CSS, and JavaScript. Your browser's job is to interpret this code and render it into the web page you see.
In essence, the browser acts as a bridge between you and the website, sending your requests to the server and translating the server's response into a format you can easily interact with on your device. Without a browser, navigating the vast ocean of internet content would be nearly impossible.

Modern Web browser make it easy to access websites, search the Web, and do just about everything online. But by default, browsers might not have all the functionality you want. In these cases, many people will customize by installing a browser extension.

A browser extension is essentially a small piece of software that performs a function or adds a feature to a browser client. Since extensions are given special authorizations within the browser, they are attractive targets for attackers.

An extension adds some custom function to your core browser. They can help you take notes, manage passwords, block ads, and more. But extensions can also introduce security risks.

At essence, Web browsers process information. Uploads from your computer, downloads from the Web, visiting websites…all this happens in your browser, with information constantly sent back and forth. Browser extensions modify this basic flow of information in some way.

An extension is a small piece of software you can install to customize your browser's appearance or function. Some extensions come from the makers of a browser, but more often, they come from third-party developers trying to add some new functionality that a browser doesn't already have

Extensions can do almost anything. They might enable email encryption, ad blocking one-click password storage, spell-checking, and more. Extensions are like specialized agents working with the flow of information through your browser. They might organize your notes, protect you from hackers, or just transform how that information appears in the browser window (e.g. dark mode).

But in order to function, extensions usually need broad-sweeping permissions over your browser. Some require access to almost everything your browser sees. Everything from the sites you visit, keystrokes, even your passwords. This means a bad extension (or a poorly secured browser) can expose you and your data, and introduce major privacy and security risks.

Security and privacy risks with browser extension:

One major concern is the potential for security vulnerabilities. Poorly designed or malicious extensions could compromise data integrity and expose sensitive information to unauthorized access. Moreover, certain extensions may introduce performance issues or conflicts with other software, leading to system instability.

Many browser extensions are safe, but there's always some degree of inherent risk. Installing an extension introduces new software to your browser—software which could potentially have security weaknesses (or be downright malicious).

Third-party extensions might secretly include malware, or have security flaws that hackers can exploit. And it's very common for attackers to "spoof" legitimate browser extensions, creating fraudulent versions to trick and defraud users (e.g. the numerous Meta Mask fakes on the market).

There’s even a risk in downloading from trusted channels like the chrome web store sometimes Google will accidentally remove the authentic version of an extension and leave a fake one behind. It’s also possible for a legitimate extension to make it onto the Web Store, and then be sold to a different publisher who changes the code and introduces malware.

And, with broad permissions over your browser, malicious extensions can cause all kinds of harm. For example, malicious extensions have been found to secretly use the browser to click on pay –per- click ads ,collect user data ,intercept data from Gmail and—most recently—hijack face book accounts using a fake chat GPT extension.

Guide to use extensions (more) safely

Many extensions are safe and reputable, you just have to be careful when installing and using them. This guide covers the most important considerations when using extensions.

Even though extensions can be risky, if used correctly, they can be extremely beneficial. It’s ***especially*** important to research extensions if you are using an application that accesses **P4 protected data**.

Before Installing an Extension:

To validate the safety of any extension, start with a few quick checks:

- Check out the developer’s website to see if it’s a legitimate extension and not a one-off by an unvetted source.
- Read the description. Look for things that may be questionable, like tracking info or data sharing.
- Check out the reviews. Look for users complaining of oddities happening, speculating on their data being taken, or for anything that strikes you as odd.

When Installing an Extension:

- Be picky. The more extensions installed, the bigger the attack surface you open up to attackers. Only pick the most useful and delete the ones you don’t need.

- Only install through trusted sources. While not guaranteed safe, security technicians review extensions for malicious content.
- Review permissions. Review extension permissions closely. If an extension installed suddenly requests new permissions, be wary. If you can't find a reason for the permission change, it's probably better to uninstall.
- Use antivirus protection. Install and run **System Center End Point Protection (SCEP)** to detect and neutralize malicious code in browser extensions.

Don't overload your browser with extension:

- Every extension you install adds a security risk and a performance burden to your browser. If you've got 15 extensions installed—and running—you'll likely see a slowdown in browsing and even device processing speeds. Everything will just move slower, or your computer's fan might even turn on more.

  Know what extensions you have installed:

  Its best practice to monitor the extensions you've installed, and which are still actively running in your browser or on your device. Then if you hear about a risky extension or a possible data leak, you know to take action.

Delete unused extension:

Finally, you should delete any extension you're not regularly using. If it's not in daily or weekly use, it's probably not worth keeping on your browser. When you look at your list of installed extensions, you might find more there than you thought. If you're unsure how an extension got installed or where it came from, delete it.

Depending on your device and browser type, you'll have different extensions available, and different official resources to download from.

2) Securing Your Browser: Best methods & their trade-offs for a safer browsing experience.

Today world the internet is a vast and wonderful place full of information, entertainment, and opportunity. However, with all that the internet has to offer, it can also be a dangerous place if you're not careful; especially in recent years, with the exponential increase in cybersecurity threats and breaches. Malicious emails, viruses, and inappropriate content are only a few of the potential threats to prevent when browsing online. So whether you’re a first-time web surfer or an experienced pro, read on for some well-tested tips on how to browse the internet safely!

Why Secure our Browser

A Web browser is one of the most frequently used software components on your PC. Therefore, it makes perfect sense to practice good **Web browser security**. As a general rule, most Web browsers that accompany your PC's operating system come without the security features set up. It is left to the user to set up the configuration to create a secure Web surfing environment.

Failing to secure your Web browser can encourage unscrupulous hackers to easily take control of your PC. By not securing your Web browser, you are opening up your PC to spyware and adware programs, viruses, and other attacks with malicious intent.

About Vulnerable Web Browsers

Most Web browser software comes pre-installed on your PC's operating system. The common Web browsers are Internet Explorer, Apple Safari, and Mozilla Firefox. The fact that there are three popular types make it easier for hackers to focus on vulnerabilities and then exploit them with malicious software attacks.

Malicious attacks take advantage of the following:

- A lot of Web surfers neglect to configure their Web browser security settings or do not understand how to do this.
- Many users view enabling and disabling certain functions as a hassle so they do not take these security measures.
- The average Web surfer clicks on ads and links without thinking about the reputation of the website or the consequences of their clicking habits.
- Web browser users tend to concentrate on all of the advantages that are highlighted by the Web browser creator and do not consider what effect these improvements have on the overall security.
- New PCs with Web browsers pre-installed usually contain other types of software bundled together. Although the software seems like a good deal, the PC user does not realize that the additional software increases the vulnerabilities to attacks.

- Many websites encourage the download of added tools to enhance the browsing experience such as Plug-Ins, Java, ActiveX, and other related software. While these tools enhance the browsing experience, they also increase the vulnerability of your Web browser.
- New vulnerabilities are always discovered once a Web browser has been released to the public. Until there is an upgrade to counteract the problem, the Web browser is vulnerable and open to software attack.

These are only a few reasons why you should secure your Web browser. The process of configuring your browser security features is rather simple to accomplish and well worth the investment of a few minutes of your time.

Due to the explosion of the Internet, attacking the vulnerabilities in Web browsers has become one of the most popular ways for intruders to take over your computer, steal your identity and passwords, spy on your surfing habits, and in the worst cases, destroy your computer altogether.

Best methods of securing our browser:

Updated Browsers and Plugins Go a Long Way

No matter what device you use, your first point of contact with the internet is usually a web browser. Developers constantly release new versions to ensure you can enjoy the most recent advancements on the web, which include utilizing HTML5 video and audio, complex styling, and enhanced performance. However, because of compatibility and security issues, several websites have stopped supporting previous versions of their sites.

Consequently, the lack of support acts as an access point for hackers. Hackers frequently target web browser flaws, which is why software manufacturers offer frequent updates to fix any issues. Installing the most up-to-date versions on your system helps protect your browser and personal data.

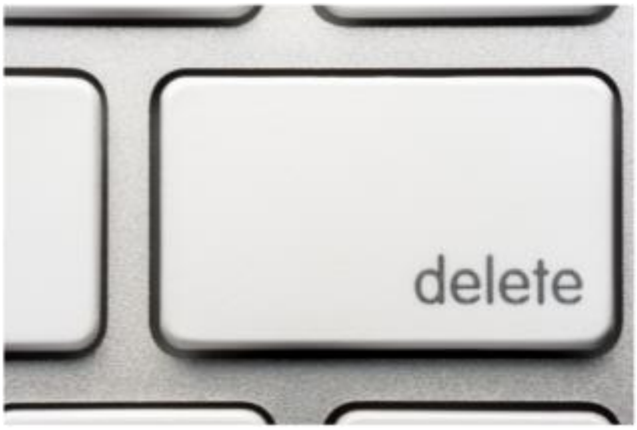
Be Mindful of the HTTPS

HTTP is a computer protocol that isn’t encrypted. On the contrary, HTTPS is secure. When browsing the internet, it is important to ensure the website you are entering starts with ‘HTTPS’. The ‘S’ stands for “secure” and is based on the Secure Sockets Layer (SSL). Browsers transmit information through HTTPS regardless of whether you want them to or not. However, SSL encrypts the link so that unauthorized users who may try to access your data won’t be able to decipher it, rending your information useless (and safe).

Signs to look for: Always ensure your url starts with HTTPS. In addition, look for the lock symbol on the left side of the web address: A secure connection implies a lock sign, while an exclamation point indicates that access is not safe; the site isn’t using a private connection if it uses the info sign.

Clear Cookies and the Web Browser Cache

Although websites monitoring your online activity is inevitable, there are ways to minimize the amount of information they monitor and track. By cleaning your browser’s cache, the information automatically stored on your device when visiting new sites will be deleted. In addition, deleting any cookies will erase all previous activity, information, and settings on your device. By doing these on a regular basis, you can prevent advertisements from tracking you across the internet and protect your information.



Clearing your cookies and cache can be done manually in all modern browsers, and it’s a quick and simple process. However, there are also computer solutions that automate the procedure to make your life simpler. It may be worth considering whitelisting sites that you use on a regular basis so that you don’t have to re-enter your login credentials repeatedly.

Not Everything You Download is Safe

Games, applications, images, music—the possibilities to download entertainment are endless on the internet. They’re amusing and, at times, provide us with excitement. However, downloading content from the internet can be unsafe and caution must be taken. Its best practice not to download apps or attachments frivolously as it may be a vector for infections such as viruses or malware.

Moreover, downloading from unreliable sources (i.e. unfrequented sites) may lead to a nasty surprise. Data breaches, identity theft, and viruses are only a few of the unfortunate consequences of downloading from unreliable sources. Therefore, download your programs only from trustworthy places. You should also scan files for viruses before clicking on them. If you’re concerned about a file being harmful to download, you can cancel the procedure in the download toolbar before the download has completed.

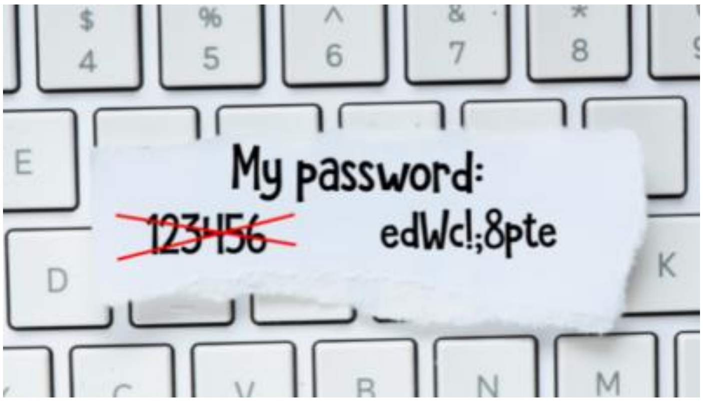
Install Antivirus and Firewall Protection

Regardless of how carefully you browse the web or how knowledgable on malicious vs safe links you may be, you need antivirus and firewall protection software on your computer. 95% of cybersecurity breaches are due to human error and it can be easily prevented with easy-to-install software.

Even in the most trustworthy of websites or files, threats may be hidden. Installing competent antivirus software is well worth a little investment of time to protect yourself online. Fun fact: The most trustworthy antivirus software on the market now uses big data and AI to monitor each running program and detect assaults before they occur, meaning your computer is safer than ever.

Impose Strong Passwords with a Password Manager

According to a recent Verizon Data Breach Investigations Report, nearly 80% of data breaches are caused by poor password management. Creating weak passwords and re-using passwords for multiple sites are the most common mistakes people make online. Unsurprisingly, the more secure your password is, the less likely you will be a cybercrime victim. The best practice for creating strong passwords is to avoid using dates, phone numbers, favourite films, or sports team names as passwords. Alternatively, a strong password should be complex– lengthy, unpredictable, and contain special characters, symbols, uppercase letters, and digits (ex. %FolLow Us!).



On top of having strong and lengthy passwords, the remaining issue is remembering them which could prove to be exceptionally difficult, but that's where a **password manager** comes in. They encrypt and safeguard your login details for every website you visit, allowing you to log in automatically and free you to focus on the one main password

Use Two-Factor Authentication (2FA)

Two-factor authentication, also referred to as multi-level authentication, is considered on the safest methods for securely using the internet. **Two-Factor Authentication (2FA)** increases the security of your online accounts during the login process. 2FA requires users to enter personalized security questions in addition to providing passwords to login.

Even if your password is guessed by cybercriminals, they will not be able to log into your account with knowing personal information about yourself that is not commonly known or searchable. An added level of protection like 2FA makes it more difficult for hackers to gain access to your accounts.

Use a VPN

Proxy networks, also known as VPNs, encrypt your online presence allowing you to maintain your anonymity. Public networks, like Starbucks free Wi-Fi, can be dangerous because hackers can use these unsecured networks to plant malware on your device. We know it would be silly to convince you to stop using free publicWifi, so instead, recommended to use VPN

By installing a VPN, you can essentially turn a public network, private, through masking your IP address. Encrypted information is then sent to the VPN server, which decodes requests and transmits them to their intended destination. The data is sent back through the same channel, preventing websites, advertisers, and internet service providers from monitoring what you do, making your online activity untraceable. You can easily buy a VPN online, with popular companies like Norton.

Ad Blocker is Your Friend

The popularity of ad blockers has risen in recent years. The high demand can be attributed to the increasing presence of pop-up advertisements on websites and targeted advertisements following us around the internet. They're annoying and since they can be removed, why not do it? Ad blockers prevent websites from displaying advertisements by reading a sites "script" and determining whether the user has added a filter to block ads on that site. As the website loads, the ad blocker takes effect and blocks the advertisements before the page has fully loaded (it's really that fast).

Ad blocker is your friend. However, if you want to support your friends online, make sure to whitelist your favourite websites. Ad blockers have been semi-controversial due to the consequences they may have on businesses. Many websites are paid for through advertising, which is a pay-per-impression business model. If you have an ad blocker on, you are denying the author their revenue stream, since it's based on impressions. By all means, use an ad blocker to protect yourself, but remember to whitelist your favourite destinations since the ad income is what keeps them going!

Make Use of the "Do Not Track" Feature

The majority of modern web browsers have the ability to send a "do not track" request to websites. Do not track (DNT) is a browser privacy setting that allows users to send a request to websites asking them not to track their activity. When you send a request, an HTTP header is added to all of your web traffic which lets analytics services, social, and advertising networks know you do not want to be tracked.

Although this is a great tool, websites still have the ability to decide whether to accept your request. In most cases, websites and servers do not alter their behaviour and appear to disregard DNT requests. However, there's no harm in enabling the feature and making it clear you don't want to be tracked. When it comes to browsing the internet safely, everything helps!

Cybercriminals are on the lookout for methods to obtain your data. One little mistake might cause you a lot of stress, financial loss, and even reputational damage. Safe internet surfing, however, is possible. In this article, we provided you with well-tested tips and secure web browser security techniques for navigating the internet safely. Now it’s time to take your security and privacy into your hands with these tips!

3) Two-Step Authentication: Compare methods, strengths, weaknesses & choose the right one.

Along with the first digital devices rose a need to ensure the security of stored data and to differentiate access to various functions. A variety of methods for unambiguous authentication of users on which security is based are called authentication factors. These include codes, logins, passwords, certificates, hardware keys, and so on. The whole set of authentication factors can be divided into three groups:

- Factors of knowledge (something known to the user);
- Ownership factors (something that the user owns – documents or items characterized by some unique information (usually these factors boil down to “devices”, although this narrowing is not always justified));
- Biometric factors (physical characteristics of the user).

There is a huge variety of authentication factors, not all of which are equally convenient and safe. In order to raise the security level of the authentication process, **multifactor authentication** is used, in which several authentication factors of different types are used to verify access. The disadvantages of some factors can and should overlap by the merits of others. Despite the greater security, the more authentication stages are used, the more effort and time it takes to **authorize**. According to the combination of characteristics, two-factor authentication is considered the most optimal today by the combined security, convenience and applied effort characteristics.

Currently, most authentication methods rely on knowledge factors, such as a traditional password, while two-factor authentication methods add either a possession factor or an inherence factor.

Authentication factors, listed in approximate order of adoption for computing, include the following:

- A **knowledge factor** is something the user knows, such as a password, a personal identification number (PIN) or some other type of shared secret.
- A **possession factor** is something the user has, such as an ID card, a security token, a cell phone, a mobile device or a smartphone app, to approve authentication requests.
- A **biometric factor**, also known as an **inherence factor**, is something inherent in the user's physical self. These may be personal attributes mapped from physical characteristics, such as fingerprints authenticated through a fingerprint reader. Other commonly used inherence factors include facial and voice recognition or behavioural biometrics, such as keystroke dynamics, gait or speech patterns.
- A **location factor** is usually denoted by the location from which an authentication attempt is being made. This can be enforced by limiting authentication attempts to specific devices in a particular location or by tracking the geographic source of an authentication attempt based on the source Internet Protocol address or some other geolocation information, such as Global Positioning System (GPS) data, derived from the user's mobile phone or other device.
- A **time factor** restricts user authentication to a specific time window in which logging on is permitted and restricts access to the system outside of that window.

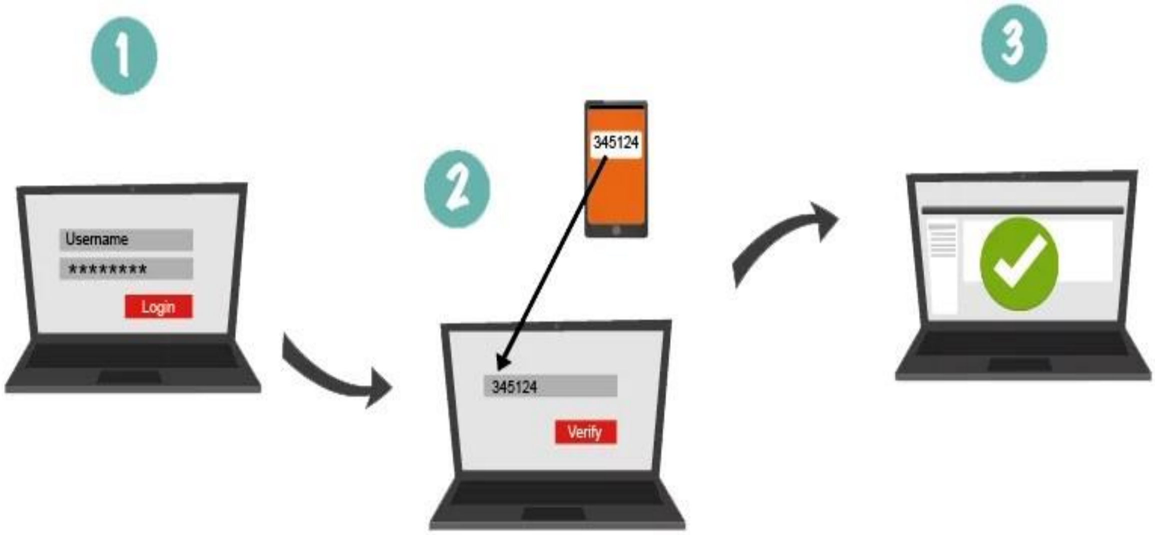
The vast majority of two-factor authentication methods rely on the first three authentication factors, though systems requiring greater security may use them to implement multifactor authentication (MFA), which can rely on two or more independent credentials for more secure authentication.

Two-Factor Authentication

Two-factor authentication (2FA) is one of the most reliable types of the user authentication nowadays, used to obtain the rights to access any resource or data (from mailboxes to bank card payments). Two-step authentication is a much more reliable alternative to the traditional one-factor authentication (1FA) with the help of a login-password pair, the security of which is quite low currently. There are a huge number of methods for hacking and circumventing password authentication, from social engineering to distributed brute forcing, based on pre-organized botnets. In addition, some users use the same password to log into all their accounts, which in turn further simplifies the access of scammers to protected information and transactions. The main advantage of two-factor authentication is the increased login security. As for the shortcomings, the main two being the increase in the time of entry into the system and the risk of losing the physical media serving to pass one of the authentication steps (mobile phone, U2F key, OTP-token). In this article, we reviewed several of the most convenient and secure second authentication factors for use in 2FA.

SMS Codes

SMS codes generated by special services are the most common kind of factors used in the **mobile two-factor authentication**. It is quite convenient (most modern users always keep their smartphones on them) and does not take much time. In addition, this check is in most cases effective, for example, to protect against automated attacks, **phishing**, password brute forcing, viruses, and the like.



But in case someone is intent on hacking you, bypassing SMS authentication is possible. After all, usually the phone number tied to the account is not a secret (as a rule, it is the same contact number that can be found from your friends, social network or business card). Having received personal information of the owner of the number, scammers make a fake identity card and use it at the nearest office of the mobile operator. Despite the fact that in some countries the legislation requires a complete reconciliation of the ID data, SIM can be authorized for the reissuing by the most ordinary employee, not particularly bothering to verify the authenticity of the document. Thus, a new card with your number is created (in turn, the previous SIM is blocked) and the scammer gets the opportunity to pass the second stage of authentication. The second drawback is that some state authorities (for example, police) can ask the mobile operator for access to your cellular number (including SMS). This is done in real time, and even if you are eavesdropped on, you will not even know. On the other hand, SMS messages will help you find out that someone is trying to hack your account and change the password or the attached phone number in time.

Pros:

- Simplicity of the usage – the user just needs to input the code from the SMS that came to their mobile phone;

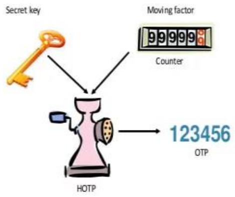
- In case an attempt to hack your account happens, you will immediately know about it, as you will receive a message with a one-time password (OTP) and can immediately change your account password.

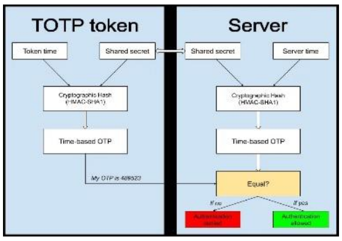
Cons:

- Need to pay SMS sending fees. This con is especially important for the companies protecting their user. In B2B segment it’s more advantageous cost-effective to use software or hardware tokens.
- Cannot be used in case of the absence of the cellular coverage (on remote territories or abroad) or telephone itself (theft, loss, battery discharge).
- SIM swap opportunity allows attackers to steal the phone number.
- SMS messages can be intercepted with a variety of methods.

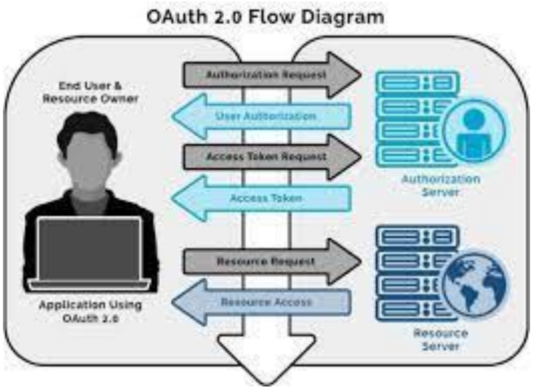
Code Generation Applications

Code generation apps are a worthy alternative to SMS codes. The most common among such applications is the Google two factor authentication solution – Google Authenticator. Such software OTP tokens generate codes independently based on a particular algorithm or random sequence. The main algorithms for generating such one-time codes are the HOTP (hash-based one-time password, RFC4226), TOTP (time-based one-time password, RFC6238) and OCRA (OATH challenge-response algorithm, RFC6287) that were developed and are supported by the OATH (Initiative for Open Authentication).





HOTP (hash-based one-time password) and TOTP (time-based one-time password) shown above and OCRA (OATH challenge-response algorithm) shown below



Pros:

- The main advantage of such two-factor authentication software is the possibility of using in the absence of the cellular coverage or the access to the Internet.

Cons:

- Need to use a smartphone or other similar device;
- Application can be hacked;
- Smartphone battery can discharge;
- If the smartphone is factory reset or lost, or authenticator application is deleted accidentally, the token would be lost and its recovery is a great pain.

U2F Tokens

U2F is an open standard for universal two-factor authentication (2FA), developed by the FIDO Alliance with the participation of such world-famous corporations as Google, PayPal, Lenovo, MasterCard, Microsoft, NXP, Visa, etc. According to the creators' idea, authentication through this protocol is carried out with a help of a hardware module, in the role of which a physical medium – USB tokens (the most common devices are YubiKey) – are used. These devices are equipped with special software and a digital key at a manufacturing stage. The USB key is simply inserted into the corresponding desktop or laptop connector. This authentication factor operates as follows:

- The user is authorized on the website/in the application using a login-password pair.

- The server checks the credentials and, if they are correct, requests the signature (generates a challenge) for the token and returns it to the user program (usually it would be a browser).
- The program transmits the challenge to the token, which, after confirmation from the user (for example, a press of a token button), returns the one-time password generated according to the certain algorithm.
- The program sends a response to the server.
- If the answer is correct, authentication takes place.

Pros:

- No need to connect to a cellular network or the internet, because all the necessary data are already stored at the device.
- Ease of use – just connect the token to the USB port and press a single button when requested.
- There are Yubikey token models with two slots, which allows using them to access two websites instead of one.

Cons:

- Low prevalence, because the standard is still quite new. Currently, U2F tokens are supported by Gmail, Google Accounts, GitHub, Dropbox, Last Pass and WordPress.
- U2F USB tokens, at the moment, are compatible only with the Chrome browser since version 38. This restriction is applied not by Yubikey tokens, but the U2F standard itself.
- Many companies block operations with USB ports on corporate computers.

- U2F devices are created to access 1 or 2 specific resources; an active Internet user will need to store a bundle of devices for the access to different websites.
- U2F devices are relatively costly: prices for the cheapest models start from $20.
- The token is easily forgot inserted into computer when going away from a workstation. Some people also leave them inserted all the time for the convenience, which undermines the whole concept of 2FA.
- USB connection itself leaves the opportunity of some kind of malicious code injection and Trojans.
- It is desirable to buy tokens in pairs in case of loss.

Contactless Hardware Tokens

A worthy alternative to the previous authentication method are contactless hardware tokens. Why do we consider this variant of tokens to be the most reliable second factor:

- They are standalone, unconnectable devices which eliminates the possibility of unauthorized external or remote access by hackers;
- They are invulnerable to the injection of malicious code;
- They allow creating a true two-factor authentication that separates something you have (a token) from something you know (a password);
- They are immune to the danger of a SIM card theft, secret key exporting, catching a virus which intercepts one-time passwords;
- Their batteries last for years, so you will never face the discharge problem during a service term;
- They do not need a cell network signal or roaming to work.

There are 2 types of contactless hardware tokens available on the market today:

1. The common models with pre-installed secret keys (seeds). This is a good option if offered directly at the resource that employs the 2FA user account protection. For example, such hardware tokens are proposed by Blizzard, PayPal and AdvCash. And probably you already have similar tokens for the access to your online banking.
2. But what if the website does not offer its own contactless hardware tokens? In this case, recently released programmable hardware tokens would be a great help. These devices can be flashed through the NFC Protectimus Slim NFC using the Protectimus TOTP Burner application for Android smartphones. These OTP tokens are compliant with Google Authenticator authentication server standards (32 symbols long secret key (Base32) and 6-digit OTP). Among resources that implement this standard are Facebook, Google, Dropbox, GitHub, Kickstarter, KeePass, Microsoft, TeamViewer, and many others.

The use of one-time passwords

Amid the constantly growing online business segment, data protection has to be particularly reliable. If you still can 'survive' the hacking of your personal page on social networks (though it's extremely unpleasant too), the loss of business information can lead not only to the loss of reputation and income but even to the closure of the company.

One of the most defenceless points in the information security is the reliable user authentication of everyone attempting to access his or her account on a particular website.
Common reusable passwords are well known to everyone and are pretty useless at the present level of hacker threats. They are unable to withstand the pressure of attackers, equipped with such 'tools' as key loggers, interception of the data, and methods of social engineering. Much higher level of protection can be provided by using one-time passwords.

How one-time passwords are generated

The most convenient and secure one-time passwords generation tool at the present moment is a token. It can be either a software token – an application for a tablet or Android/iOS smartphone or hardware token in the form of USB flash drive, trinket or credit card. For extra protection, each token can function along with the PIN-code, which should be used while entering the one-time password.

One-time passwords are usually generated by using one of three algorithms:

1. **HOTP** – HMAC-based one-time password algorithm. Server and OTP token keep count the number of authentication procedures performed by the user, and then generate the password, using this number in the calculations. The mismatch in the calculations between the server and the token may cause a problem. Such situation is possible, for example, if the user repeatedly presses the button for generation of an OTP password and doesn’t use the password later.
2. **TOTP** – time-based one-time password algorithm. In this case, the password is created taking into account the internal clock of the token. TOTP is convenient, because the time of OTP password’s functioning is limited, which means it can’t be created in advance or used after the expiration term.
3. **OCRA** – OATH challenge-response algorithm. This is a very reliable algorithm, assuming, however, a bit more steps than the previous ones. The mutual authentication of the user and the server occurs during its work. Unlike other algorithms, it uses a random number issued by the server as an input.

It is worth mentioning that if you use the TOTP and OCRA algorithms, sort term passwords are produced, which significantly complicates the process of hacking.

Threats and risks of using one-time passwords

No matter how reliable is the two-factor authentication with the one-time passwords, there are some dangers, which can be avoided, if you take care of the precautions.

- **Interception of the OTP password**. In this situation, which is often called ‘a man in the middle attack’, a hacker intercepts the authorized password and authorizes in the system. To avoid this, you can use 2FA with data signing function (CWYS), available in Protectimus SMART token. It allows considering not only the password, but also some other parameters of the particular transaction during the authentication: place of the access to the network, browser, system language, and so on.
- **Loss of the token**. In order not to shed bitter tears in the case of loss or theft of the token, you should foresee an obligatory use of PIN-code at the time of using the device.
- **Attempts to hack the PIN-code**. The solution, in this case, is special settings according to which the OTP token will be blocked if the wrong PIN is repeatedly entered.
- **Hacking of software token**. A hacker can copy the software token and attempt to find the secret key used to generate the OTP. A method of protection is the use of the PIN-code as one of the values in the generation of the one-time password. Thus, even knowing the secret

key, a hacker can’t create a password, because PIN-code is not stored in the software token.

- **A villain among the friends**. The sad situation can take place, when a malefactor and a person, who releases two-factor authentication tokens is the same person. Such person can create duplicates of software authentication tokens and use them to log in under the name of the legitimate user. To prevent this, the user must take part in the process of activating the software token.

It is undeniable that the two-factor authentication with the help of OTP tokens, which generate the one-time passwords, is the best authentication method nowadays. It allows you to eliminate the risks associated with the use of a standard password authentication and reliably protect the data of companies and individual users.

Contactless Hardware Tokens with Pre-Installed Seeds

These OTP tokens are well-known and have been considered the most reliable one-time password generation tools for years. So why they are not so widespread as SMS confirmation and software authenticators? Mostly because shipping the devices worldwide is costly and requires notable labour resources or the cooperation with Logistics Company, which may be extremely inconvenient for smaller enterprises. Besides, hardware tokens are not free and many companies don’t consider them cost-effective, thus saving on the security of its users. Though some websites offer their users to purchase such tokens themselves, thus providing an opportunity to protect the account reliably.

Pros:

- Contactless device, protected from any possibility of malware injection;
- One-time password is generated by the device itself, which reduces the possibility of intercept to a minimum;

- Does not require network connection of any kind;
- Built-in power source is enough for years of independent operation;
- The cheapest amongst all hardware tokens.

Cons:

- If a token is compromised, then you only need to order a new one (Protectimus Slim NFC can simply be reflashed);
- If you stop using the service, then the money was wasted, there is no possibility to use it with another service;
- If you need to protect several accounts (or accounts at different resources), you will need a separate token for each. This may lead to a bundle of varying devices which may be uncomfortable to carry around (this is also true for YubiKey, but a few slims do not take much space);
- The secret key in such tokens is pre-flashed at the factory, then passed to the supplier, then transferred to the website owner. Of course, keys are transmitted in encrypted form, but there remains a tiny possibility that at some stage an unscrupulous employee or a hacker will leak secret keys. In this respect, the Protectimus Slim NFC wins unconditionally. It is flashed by the user from their personal smartphone with a secret key that is known only to them.

Programmable Hardware Tokens Protectimus Slim NFC

The main purpose of this token's creation was to obtain a more universal and safe replacement to OATH-compliant code generation applications, such as Google Authenticator, Authy, Protectimus Smart, etc.

Pros:

- The main advantage of such two-factor authentication solution lies in the fact that the token can be flashed an unlimited number of times upon changing the secret key. Thus you may use it on the websites that offer only mobile authentication, change the secret key if necessary, as well as reassign it to another service if you wish.

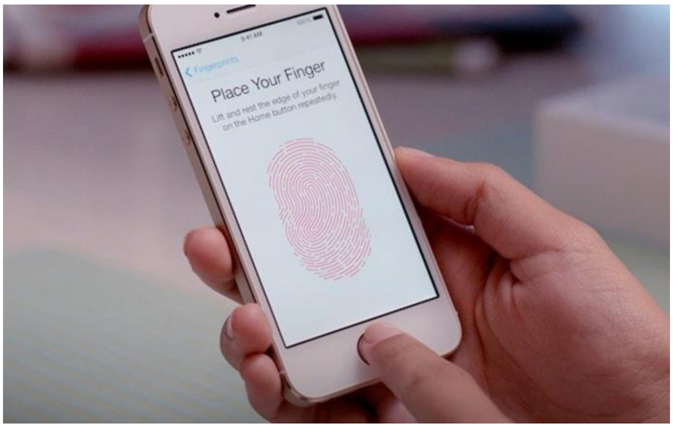
- High level of security, since the contactless token is invulnerable to malicious code injections.
- There is no need to connect the token to any port, hence no need to disconnect it when moving away from the workstation.
- Ability to change the secret key and reflashing the token takes only three minutes.
- More versatile and less expensive, in comparison with U2F keys option (up to 40% difference in price when characteristics are comparable).
- You can order custom branding even when ordering the single token.

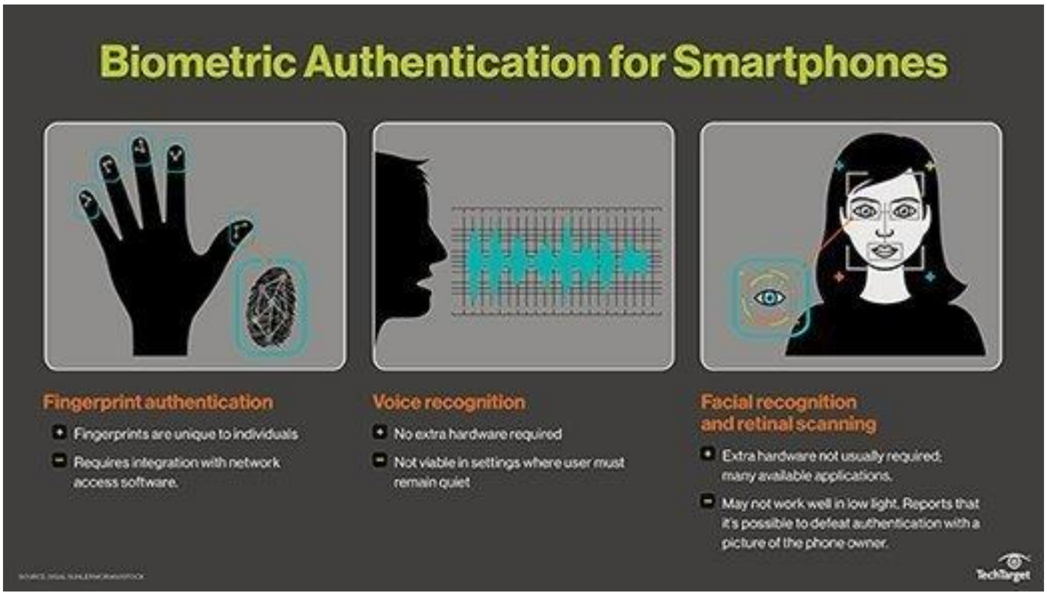
Cons:

- The built-in battery lasts about five years, after which the token needs to be replaced.
- Some restrictions on the size of passwords (only secret keys with a length of 16 to 32 characters in Base32 encoding are allowed), the built-in display for the challenge signature is six positioned (the standard supported by Google Authenticator). This makes such a token inapplicable to resources that employ secret keys shorter than 16 and longer than 32 characters, and eight-character one-time passwords, although such are rare.

Biometric Data

This authentication method uses biometric user data – fingerprints, facial features, eye iris or voice recognition. Undoubted advantage of this method is its unmatched convenience. You just scan a respective body part and get access. Nevertheless, currently, biometric scanners are not accurate enough to serve as reliable second factor despite being promoted as such by industry giants like Google, Samsung, and Apple. And if your biometric data is not recognized, you have to enter the recovery password which effectively defeats the whole purpose of two-factor authentication. Moreover, if your biometric factor, iris, for instance, was compromised once, it cannot serve an authentication factor anymore. Even if currently hacking the biometric scanners is hard, it is still possible and will become easier with time.


Fingerprints
Place Your Finger
Lift and rest the edge of your finger on the Home button repeatedly.



Biometric Authentication for Smartphones

Fingerprint authentication

- ⊕ Fingerprints are unique to individuals
- ⊖ Requires integration with network access software.

Voice recognition

- ⊕ No extra hardware required
- ⊖ Not viable in settings where user must remain quiet

Facial recognition and retinal scanning

- ⊕ Extra hardware not usually required; many available applications.
- ⊖ May not work well in low light. Reports that it's possible to defeat authentication with a picture of the phone owner.

TechTarget

Pros:

- Convenience for the user;
- No need for physical media;
- No need to connect to any networks.

Cons:

- Extremely high cost of implementation and deployment;
- To date, the risk of inaccurate recognition is still quite high (meaning that the system can deny access due to an erroneous determination of the

user’s biometric parameters). For example, the pattern of the fingers can easily be damaged by common cuts; in addition, there is a category of people – with features of temperature and body moisture – for which it is very difficult to take the print;

- If a biometric factor is compromised once, it cannot be used anymore.

The most budgetary and easy to implement is **SMS authentication** or special **applications** for one-time passwords generation. If the need for confidentiality is very high, **contactless tokens** are most suitable for you, which, on the one hand, do not store any of your personal data (such as biometric information), and, on the other hand, are unique and not subject to hacking (except someone steals the device itself, which, however, can be countered). As for **biometrics**, its implementation is reliable only in the case when some reserve method of identification is envisaged, and it requires quite significant financial investments.

One thing should be noted firmly though – 2FA solves the problem that arises when one of the authentication factors is compromised. However, if both factors are on the same device, then there is really no two-factor authentication. To ensure an appropriate level of security, both factors must be from different groups or implemented from different devices.

4) Strong Passwords: What makes them weak, how attackers exploit them & how to create secure, memorable ones?

You'll need to **create a password** to do just about everything on the Web, from checking your email to online banking. And while it's simpler to use a short, easy-to-remember password, this can also pose **serious risks** to your online security. To protect yourself and your information, you'll want to use passwords that are **long**, **strong**, **and difficult for someone else to guess** while still keeping them relatively **easy for you to remember**.

Why do we need a strong password?

At this point, you may be wondering, **why do I even need a strong password anyway?** The truth is that even though most websites are secure, there's always a small chance someone may try to access or steal your information. This is commonly known as **hacking**. A strong password is one of the best ways to defend your accounts and private information from hackers.

Tips for creating strong passwords

A strong password is one that's easy for you to remember but difficult for others to guess. Let's take a look at some of the most important things to consider when creating a password.

- **Never use personal information** such as your name, birthday, user name, or email address. This type of information is often publicly available, which makes it easier for someone to guess your password.
- **Use a longer password**. Your password should be **at least six characters long**, although for extra security it should be even longer.
- **Don't use the same password for each account**. If someone discovers your password for one account, all of your other accounts will be vulnerable.
- Try to include **numbers, symbols**, and both **uppercase** and **lowercase letters**.
- Avoid using words that can be **found in the dictionary**. For example, **swimming1** would be a weak password.
- **Random passwords are the strongest**. If you're having trouble creating one, you can use a **password generator** instead.

Common password mistakes

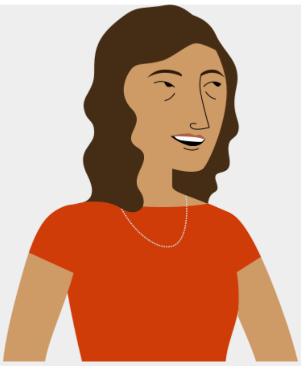
Some of the most commonly used passwords are based on **family names**, **hobbies**, or just a **simple pattern**. While these types of passwords are easy to remember, they're also some of the least secure. Let's take a look at some of the most common password mistakes and how to fix them.

Password: brian12kate5

"I doubt anyone could guess my password! It's my kids' names and ages. Who else would know that?"

Problem: This password uses too much personal information, along with common words that could be found in the dictionary.

Solution: A stronger version of this password would use symbols, uppercase letters, and a more random order. And rather than using family names, we could combine a character from a movie with a type of food. For example, Chewbacca and pizza could become **chEwbAccAp!ZZa**.



Password: w3St!

"My password is so simple! It's just the beginning of my street address with a few extra characters."

Problem: At only five characters, this password is way too short. It also includes part of her address, which is publicly available information.

Solution: A stronger version of this password would be **much longer**, ideally more than 10 characters. We could also substitute a nearby street name instead of her current address. For example, Pemberly Ave could become **p3MberLY%Av**.

Password: 123abccba321

"My password follows a simple pattern, so it's easy to remember and type on my keyboard."

Problem: While patterns like this are easy to remember, they're also some of the first things a hacker might guess when attempting to access your account.

Solution: Remember that **random passwords** are much stronger than simple patterns. If you're having trouble creating a new password, try using a **password generator** instead. Here's an example of a generated password: **#eV$pIg&qf**.

If you use a password generator, you may also want to create a **mnemonic device** to make the password easier to remember. For example, **H=jNp2#** could be remembered as **HARRY = jessica NORTH paris 2 #**. This may still feel pretty random, but with a bit of practice it becomes relatively easy to memorize.

Password: BrAveZ!2

"I use the same passwords for all my accounts. This way, I only have to remember one password!"

Problem: There's nothing really wrong with this password, but remember that you should **never use the same password with different accounts**.

Solution: Create a unique password for each of your online accounts.

Using password managers

Instead of writing your passwords on paper where someone might find them, you can use a **password manager** to store them securely online. Password managers can remember and enter your password on different websites, which means you won't have to remember longer passwords. Examples of password managers include **LastPass**, **1Password**, and **Google Chrome's password manager**.

Password: m#P52s@ap$V

"I use a password generator to create all of my passwords. They're not super easy to remember, but that's OK; I also use a password manager to keep track of them."

This is a great example of a **strong password**. It's strong, long, and difficult for someone else to guess. It uses **more than 10 characters** with letters (both **uppercase** and **lowercase**), **numbers**, and **symbols**, and includes no obvious personal information or common words. This password might even be a bit too complicated to remember **without a password manager**, which underscores why they're so helpful when creating a strong password.

Remember to use these tips whenever you create a password to keep your online information safe and secure.

5) POS Security Threats: Identify vulnerabilities & suggest solutions for malware, breaches & theft.

What Is POS Security

Point-of-sale security (POS security) creates safe environments for customers to make purchases and complete transactions. POS security measures are crucial to prevent unauthorized users from accessing electronic payment systems and reduce the risk of credit card information theft or fraud.

POS hacks represent a major opportunity for cyber criminals. POS applications contain a huge amount of customer data, including credit card information and personally identifiable information (PII) that could be used to steal money or commit wider identity fraud.

By hacking one application, malicious actors can potentially gain access to millions of credit or debit card details that they can either use fraudulently or sell to other hackers or third parties. Hackers can also exploit retailers' compromised POS applications, which can give them access to vast amounts of customer data, as well as additional applications and systems the retailer operates.

Organizations must use point-of-sale systems security to protect their applications, prevent unauthorized access, defend against mobile malware, and prevent hackers from attacking their back-end systems.

How POS Security Works

Security is one of the biggest risks of POS system environments. Hackers are constantly on the lookout for holes in security and potential weaknesses that might allow them to launch attacks on POS applications.

An attack typically begins with a hacker gaining access to a target system by exploiting a vulnerability or using social engineering techniques. They will then install POS malware that is specifically designed to steal card details from POS systems and terminals, which spreads through an organization's POS system memory to scrape and collect data. The hacker then moves data to another location for aggregation before transferring it to an external location that they can access.

Organizations can defend against these attack vectors by deploying technology that prevents POS malware. This includes whitelisting specific technology to protect against unauthorized practices, using code signing to prevent tampering, and using chip readers so customers do not have to swipe their credit and debit cards and make it more difficult for attackers to replicate card data.

Point-of-sale (POS) malware is software specifically created to steal customer data, particularly from electronic payment cards like debit and credit cards and from POS machines in retail stores. It does this by scraping the temporarily unencrypted card data from the POS's memory (RAM), writing it to a text file, and then either sending it to an off-site server at a later date or retrieving it remotely. It is believed that criminals behind the proliferation of this type of malware are mainly after data they can sell, not for their own personal use. Although deemed as less sophisticated than your average PC banking Trojan, POS malware can still greatly affect not just card users but also merchants that unknowingly use affected terminals, as they may find themselves caught in a legal mess that could damage their reputation.

POS malware may come in three types: keyloggers, memory dumpers, and network sniffers.

History

The first known POS memory scraper is RawPOS, which was found sometime in 2008. It is said to be technically simple, but can still affect modern-day card processing terminals. In April 2015, a variant of this malware surfaced, targeting devices in casinos and resort hotels in the United States, Canada, Europe, the Middle East, and Latin America.

While the industry currently detects more than 15 kinds of POS malware, no two are alike. Several of these are predecessors to new known POS malware variants. For example, Alina (aka Track), which surfaced in late 2012, is succeeded by JackPOS, which surfaced in early 2014. The Dexter variant the industry found after Alina surfaced has been succeeded by Soraya and LusyPOS. Modern-day memory scraping malware is found to be more sophisticated compared to their predecessors. Using the previous examples, Soraya is found to have the capabilities of a known banking Trojan called Zeus, while LusyPOS can communicate back to its command and control (C&C) server using Tor, a popular anonymity tool.

2014 was dubbed by industry experts as the “Year of the Largest Retail Hacks” thanks to POS malware.

Common infection method

There are two typical ways POS malware can be installed in machines capable of reading card data. First, it could be an inside job. This means that someone working in the store who has active knowledge of how the payment processing is set up can manually install the malware to target machines. Data scraped by variants that are not hooked up to a network are retrieved or accessed remotely.

Second, POS malware can be installed via social engineering or phishing lures, especially for targeted attack campaigns. It has been noted that tactics employing these come with files bearing misleading names, such as *java.exe* and *adobeflash.exe*. Such malware is known to be highly customized to fit or blend in with files associated with the target organization. Once installed, affected machines are connected to a POS botnet that reports back to a centralized C&C server.

Associated families

Here are some of the POS malware families we know of to date:

- Alina
- Backoff
- BlackPOS
- BlackPOS version 2
- BrutPOS
- ChewBacca
- Citadel
- Decebal
- Dexter
- Dump Memory Grabber
- GetMyPass

- JackPOS
- LogPOS
- LusyPOS
- NewPoSThings
- POSCardStealer
- PwnPOS
- Rdasrv
- Soraya
- VSkimmer

Remediation

Businesses that are unknowingly using affected POS machines must first of all contain the infection by disconnecting from the network and then conduct an audit to determine which terminals are infected and which ones are not. Affected POS systems are to be isolated and cleaned using anti-malware software. Once cleaned, businesses must identify the root cause of the infection and create compliance rules to prevent such an occurrence in the future. Staff hiring based on integrity plus properly training staff on fraud tactics can be beneficial for businesses.

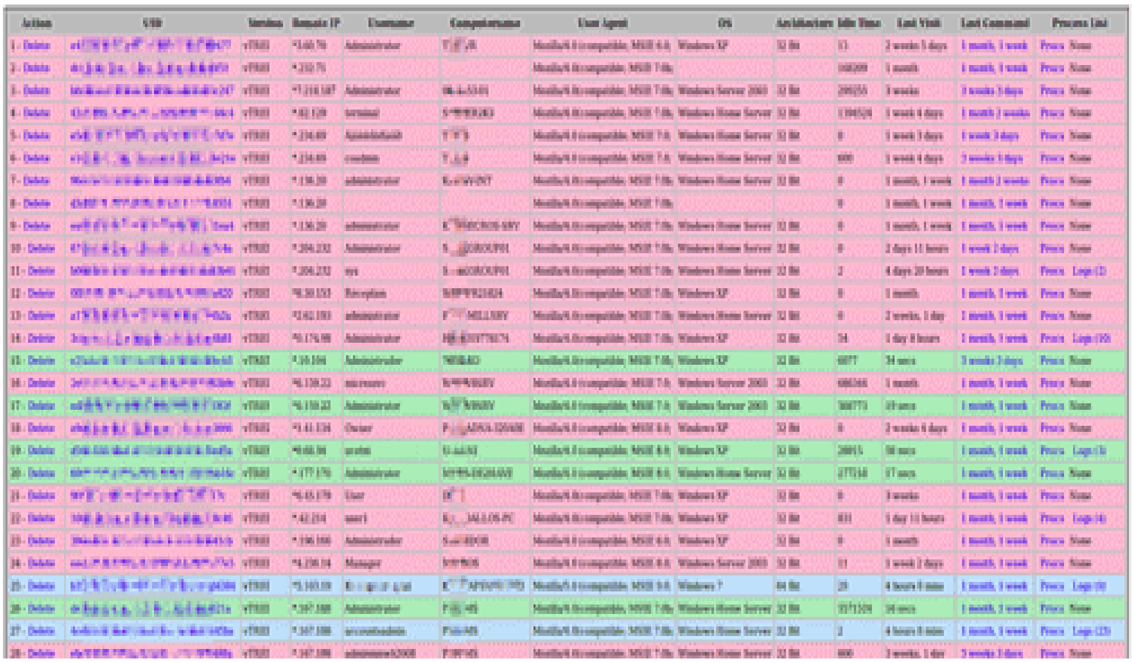
Aftermath

Big and small merchants that process debit and credit card transactions may find themselves in a pinch—worse, in court—if consumers have identified that their POS systems may be infected with malware and the merchants didn’t have ample security measures in place.

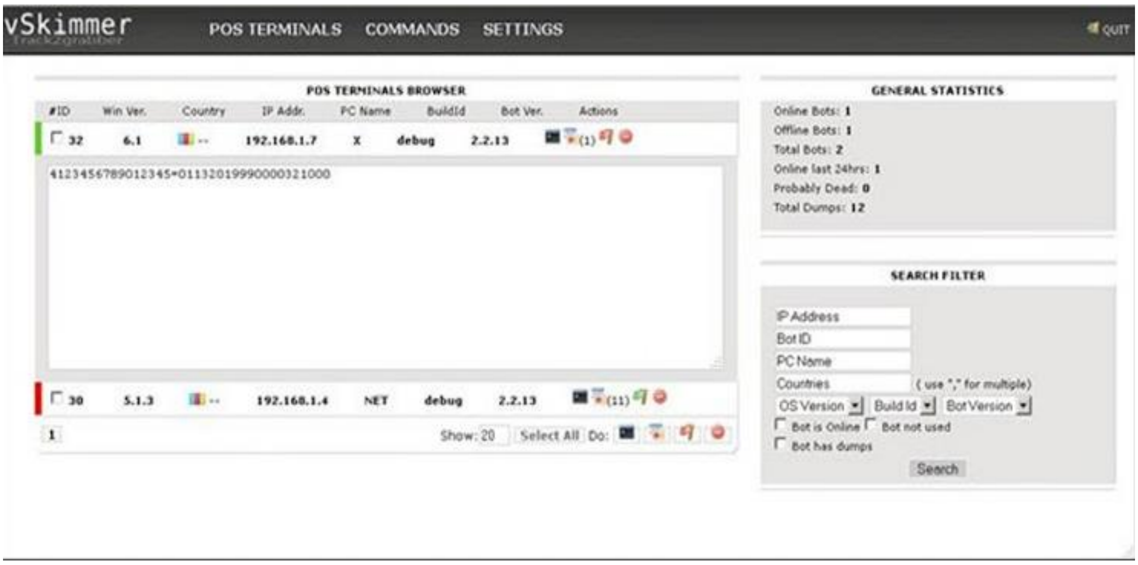
Avoidance

POS malware can be avoided if businesses have properly trained their staff to spot and correctly address social engineering lures that may allow such files to enter the business’ payment system. Introducing third-party devices to terminals and installing programs on systems connected to the network, such as browsers and games, must also be strictly prohibited.

Screenshots



Action	UID	Version	Remote IP	Username	Computername	User Agent	OS	Architecture	Idle Time	Last Visit	Last Command	Process List
1 - Delete	[illegible]	[illegible]	*3.60.76	Administrator	[illegible]	Mozilla/4.0 (compatible; MSIE 6.0;	Windows XP	32 Bit	13	2 weeks 5 days	1 month, 1 week	Procs None
2 - Delete	[illegible]	[illegible]	*.232.75			Mozilla/4.0 (compatible; MSIE 7.0b;			108209	1 month	1 month, 1 week	Procs None
3 - Delete	[illegible]	[illegible]	*7.216.187	Administrator	[illegible]-53.01	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows Server 2003	32 Bit	289255	3 weeks	3 weeks 3 days	Procs None
4 - Delete	[illegible]	[illegible]	*.82.129	terminal	[illegible]	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows Home Server	32 Bit	1198524	1 week 4 days	1 month 2 weeks	Procs None
5 - Delete	[illegible]	[illegible]	*.234.89	Administrator	[illegible]	Mozilla/4.0 (compatible; MSIE 7.0;	Windows Home Server	32 Bit	0	1 week 3 days	1 week 3 days	Procs None
6 - Delete	[illegible]	[illegible]	*.234.89	[illegible]	[illegible]	Mozilla/4.0 (compatible; MSIE 7.0;	Windows Home Server	32 Bit	600	1 week 4 days	3 weeks 3 days	Procs None
7 - Delete	[illegible]	[illegible]	*.136.20	administrator	[illegible]VENT	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows Home Server	32 Bit	0	1 month, 1 week	1 month 2 weeks	Procs None
8 - Delete	[illegible]	[illegible]	*.136.20			Mozilla/4.0 (compatible; MSIE 7.0b;			0	1 month, 1 week	1 month, 1 week	Procs None
9 - Delete	[illegible]	[illegible]	*.136.20	administrator	[illegible]MICROS-SRV	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows Home Server	32 Bit	0	1 month, 1 week	1 month, 1 week	Procs None
10 - Delete	[illegible]	[illegible]	*.204.232	Administrator	[illegible]GROUP01	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows Home Server	32 Bit	0	2 days 11 hours	1 week 2 days	Procs None
11 - Delete	[illegible]	[illegible]	*.204.232	sys	[illegible]GROUP01	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows Home Server	32 Bit	2	4 days 20 hours	1 week 2 days	Procs Logs (2)
12 - Delete	[illegible]	[illegible]	*8.30.153	Reception	[illegible]R2024	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows XP	32 Bit	0	1 month	1 month, 1 week	Procs None
13 - Delete	[illegible]	[illegible]	*242.193	administrator	[illegible]MOLLSRV	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows Home Server	32 Bit	0	2 weeks, 1 day	1 month, 1 week	Procs None
14 - Delete	[illegible]	[illegible]	*0.176.98	Administrator	[illegible]	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows XP	32 Bit	34	1 day 8 hours	1 month, 1 week	Procs Logs (10)
15 - Delete	[illegible]	[illegible]	*.10.104	Administrador	[illegible]	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows XP	32 Bit	6077	34 secs	3 weeks 3 days	Procs None
16 - Delete	[illegible]	[illegible]	*6.139.22	[illegible]	[illegible]	Mozilla/4.0 (compatible; MSIE 7.0;	Windows Server 2003	32 Bit	686346	1 month	1 month, 1 week	Procs None
17 - Delete	[illegible]	[illegible]	*6.139.22	Administrator	[illegible]	Mozilla/4.0 (compatible; MSIE 7.0;	Windows Server 2003	32 Bit	368773	19 secs	1 month, 1 week	Procs None
18 - Delete	[illegible]	[illegible]	*3.41.136	Owner	[illegible]	Mozilla/4.0 (compatible; MSIE 6.0;	Windows XP	32 Bit	0	2 weeks 6 days	1 month, 1 week	Procs None
19 - Delete	[illegible]	[illegible]	*0.68.98	[illegible]	[illegible]	Mozilla/4.0 (compatible; MSIE 6.0;	Windows XP	32 Bit	28915	38 secs	1 month, 1 week	Procs Logs (3)
20 - Delete	[illegible]	[illegible]	*.177.176	Administrator	[illegible]	Mozilla/4.0 (compatible; MSIE 6.0;	Windows Home Server	32 Bit	277118	17 secs	1 month, 1 week	Procs None
21 - Delete	[illegible]	[illegible]	*6.65.179	User	[illegible]	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows XP	32 Bit	0	3 weeks	1 month, 1 week	Procs None
22 - Delete	[illegible]	[illegible]	*.42.214	user1	[illegible]-PC	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows XP	32 Bit	831	1 day 11 hours	1 month, 1 week	Procs Logs (4)
23 - Delete	[illegible]	[illegible]	*.196.166	Administrador	[illegible]	Mozilla/4.0 (compatible; MSIE 6.0;	Windows XP	32 Bit	0	1 month	1 month, 1 week	Procs None
24 - Delete	[illegible]	[illegible]	*4.230.14	Manager	[illegible]	Mozilla/4.0 (compatible; MSIE 6.0;	Windows Server 2003	32 Bit	11	1 week 2 days	1 month, 1 week	Procs None
25 - Delete	[illegible]	[illegible]	*5.103.19	[illegible]	[illegible]	Mozilla/5.0 (compatible; MSIE 9.0;	Windows 7	64 Bit	29	4 hours 8 mins	1 month, 1 week	Procs Logs (9)
26 - Delete	[illegible]	[illegible]	*.167.188	Administrator	[illegible]	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows Home Server	32 Bit	371109	16 secs	1 month, 1 week	Procs None
27 - Delete	[illegible]	[illegible]	*.167.188	[illegible]	[illegible]	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows Home Server	32 Bit	2	4 hours 8 mins	1 month, 1 week	Procs Logs (23)
28 - Delete	[illegible]	[illegible]	*.167.188	[illegible]	[illegible]	Mozilla/4.0 (compatible; MSIE 7.0b;	Windows Home Server	32 Bit	600	3 weeks, 1 day	3 weeks 3 days	Procs None



POS TERMINALS BROWSER

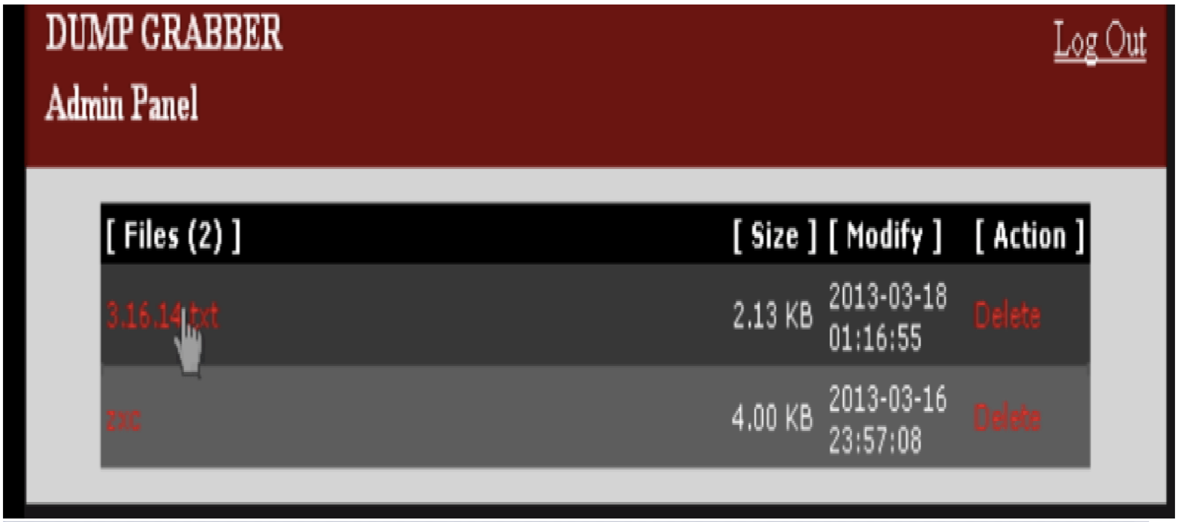
#ID	Win Ver.	Country	IP Addr.	PC Name	BuildId	Bot Ver.	Actions
□ 32	6.1	--	192.168.1.7	X	debug	2.2.13	(1)
□ 30	5.1.3	--	192.168.1.4	NET	debug	2.2.13	(11)

```
4123456789012345=01132019990000321000
```

GENERAL STATISTICS

Online Bots: 1
Offline Bots: 1
Total Bots: 2
Online last 24hrs: 1
Probably Dead: 0
Total Dumps: 12

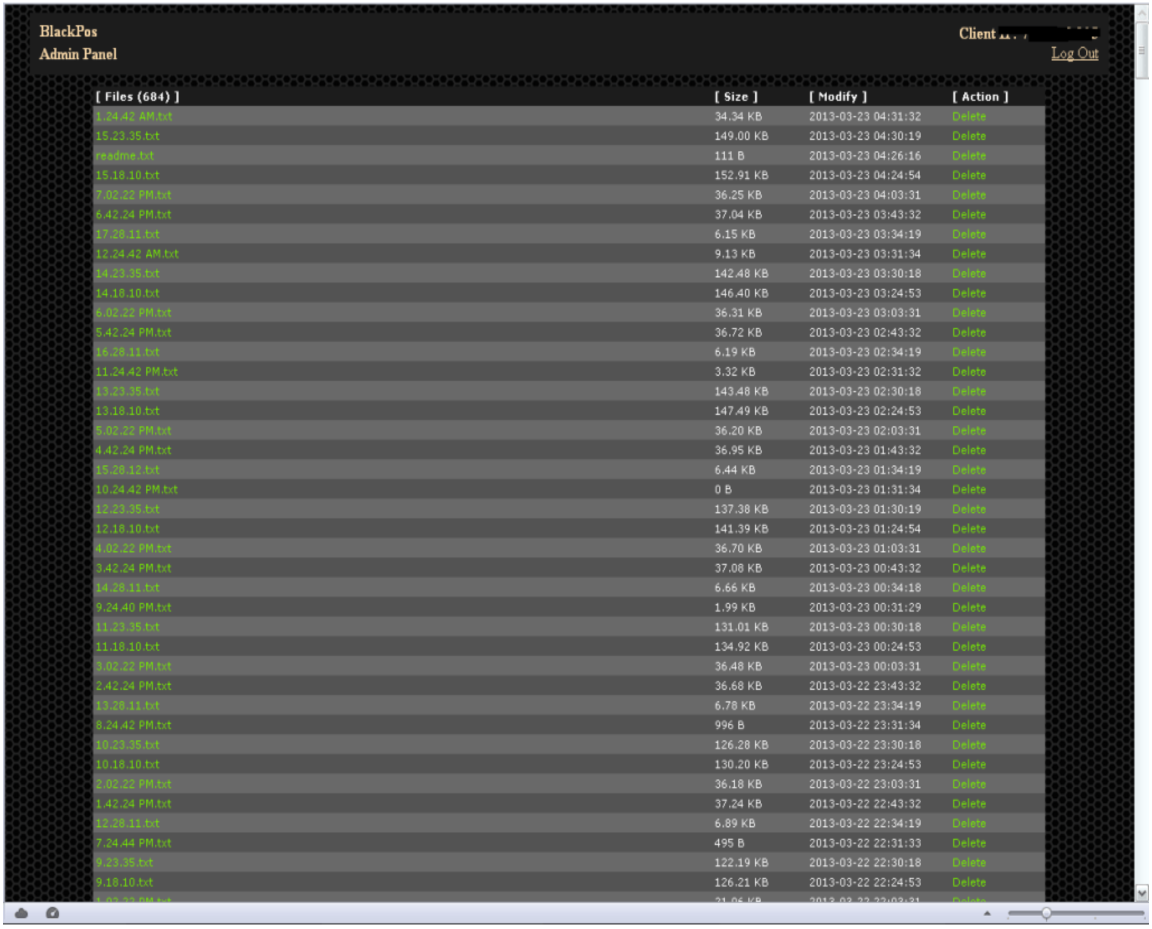
SEARCH FILTER



DUMP GRABBER

Admin Panel

[Files (2)]	[Size]	[Modify]	[Action]
3.16.14.txt	2.13 KB	2013-03-18 01:16:55	Delete
zxc	4.00 KB	2013-03-16 23:57:08	Delete



BlackPos

Admin Panel

Client [redacted]

[Files (684)]	[Size]	[Modify]	[Action]
1.24.42 AM.txt	34.34 KB	2013-03-23 04:31:32	Delete
15.23.35.txt	149.00 KB	2013-03-23 04:30:19	Delete
readme.txt	111 B	2013-03-23 04:26:16	Delete
15.18.10.txt	152.91 KB	2013-03-23 04:24:54	Delete
7.02.22 PM.txt	36.25 KB	2013-03-23 04:03:31	Delete
6.42.24 PM.txt	37.04 KB	2013-03-23 03:43:32	Delete
17.28.11.txt	6.15 KB	2013-03-23 03:34:19	Delete
12.24.42 AM.txt	9.13 KB	2013-03-23 03:31:34	Delete
14.23.35.txt	142.48 KB	2013-03-23 03:30:18	Delete
14.18.10.txt	146.40 KB	2013-03-23 03:24:53	Delete
6.02.22 PM.txt	36.31 KB	2013-03-23 03:03:31	Delete
5.42.24 PM.txt	36.72 KB	2013-03-23 02:43:32	Delete
16.28.11.txt	6.19 KB	2013-03-23 02:34:19	Delete
11.24.42 PM.txt	3.32 KB	2013-03-23 02:31:32	Delete
13.23.35.txt	143.48 KB	2013-03-23 02:30:18	Delete
13.18.10.txt	147.49 KB	2013-03-23 02:24:53	Delete
5.02.22 PM.txt	36.20 KB	2013-03-23 02:03:31	Delete
4.42.24 PM.txt	36.95 KB	2013-03-23 01:43:32	Delete
15.28.12.txt	6.44 KB	2013-03-23 01:34:19	Delete
10.24.42 PM.txt	0 B	2013-03-23 01:31:34	Delete
12.23.35.txt	137.38 KB	2013-03-23 01:30:19	Delete
12.18.10.txt	141.39 KB	2013-03-23 01:24:54	Delete
4.02.22 PM.txt	36.70 KB	2013-03-23 01:03:31	Delete
3.42.24 PM.txt	37.08 KB	2013-03-23 00:43:32	Delete
14.28.11.txt	6.66 KB	2013-03-23 00:34:18	Delete
9.24.40 PM.txt	1.99 KB	2013-03-23 00:31:29	Delete
11.23.35.txt	131.01 KB	2013-03-23 00:30:18	Delete
11.18.10.txt	134.92 KB	2013-03-23 00:24:53	Delete
3.02.22 PM.txt	36.48 KB	2013-03-23 00:03:31	Delete
2.42.24 PM.txt	36.68 KB	2013-03-22 23:43:32	Delete
13.28.11.txt	6.78 KB	2013-03-22 23:34:19	Delete
8.24.42 PM.txt	996 B	2013-03-22 23:31:34	Delete
10.23.35.txt	126.28 KB	2013-03-22 23:30:18	Delete
10.18.10.txt	130.20 KB	2013-03-22 23:24:53	Delete
2.02.22 PM.txt	36.18 KB	2013-03-22 23:03:31	Delete
1.42.24 PM.txt	37.24 KB	2013-03-22 22:43:32	Delete
12.28.11.txt	6.89 KB	2013-03-22 22:34:19	Delete
7.24.44 PM.txt	495 B	2013-03-22 22:31:33	Delete
9.23.35.txt	122.19 KB	2013-03-22 22:30:18	Delete
9.18.10.txt	126.21 KB	2013-03-22 22:24:53	Delete
1.02.22 PM.txt	21.06 KB	2013-03-22 22:03:31	Delete

Best Practices for POS Security

There are several measures that organizations can adopt and deploy to defend themselves against POS attacks and data breaches, prevent POS malware infection, and improve their POS security. Such measures include whitelisting applications, limiting POS application risks, ensuring

POS software is always up to date, monitoring activity in POS systems, using complex and secure passwords, deploying two-factor authentication (2FA), using antivirus software, and considering physical security measures.

Here are six point-of-sale best practices for improving POS security:

Use iPads for POS

Many high-profile POS attacks have occurred as a result of malware being loaded into a POS system's memory. This enables the hacker to upload malware applications and steal data without being spotted by users or retailers. But, crucially, this attack method requires a second application to be running.

As a result, Apple's iOS systems can help prevent POS attacks because the operating system (OS) can only fully run one application at any time, whereas Windows devices rely on multiple applications at the same time. Organizations can, therefore, use iPad POS solutions to run their POS systems and reduce the chances of POS attacks.

Use End-to-End Encryption

One way for customer data to never become exposed to hackers is through **encryption**. Encrypting credit card and other sensitive data as soon as the POS device receives the data and when it gets sent to the POS software server will ensure it is never vulnerable, regardless of where and how hackers install malware.

Secure Your POS with an Anti-Virus

Antivirus software allows organizations to secure their systems and prevent POS attacks. It prevents malware from infiltrating organizations' systems by scanning devices to detect anomalous or problematic applications, files, and user activity that need to be blocked or removed.

An antivirus alerts organizations when there is a potential issue and enables them to initiate the cleansing process to guarantee any present malware does not result in the loss or theft of data.

Lock Down Your Systems

The chances of employees using their organizations' POS devices to initiate an attack are relatively low, but there is a potential for **malicious insider activity** or human error. Users could steal, lose, or accidentally misplace devices that have POS software installed, which could allow anyone that picks up the device to view or steal customer data.

Organizations need to lock down their systems to avoid these risks. This involves ensuring employees lock down their devices at the end of every working day, diligently keeping track of every corporate device throughout each day, and securing devices in locations that only a few trusted individuals have access to.

Avoid Connecting to External Networks

Sophisticated hackers can compromise POS systems remotely. This is typically possible through systems that can connect to external networks, which hackers will look to infiltrate through software that remains dormant until it connects to a POS system.

Organizations, therefore, need to avoid connecting to external networks and ensure their systems remain local, internal, and secure. They should look to restrict the handling of business-critical tasks, such as transactions and payment processing, to secure corporate networks.

Be PCI-compliant

Putting measures in place to manage and protect POS systems is crucial, but organizations also need to comply with the stipulations of data privacy and protection regulations. This includes the Payment Card Industry Data Security Standard (PCI DSS), which regulates security standards for any organization that handles credit cards from major providers. Organizations must comply on all transactions carried out on card readers, online shopping carts, networks, routers, servers, and paper files.

PCI DSS is mandated by financial organizations and administered by the PCI Security Standards Council, which is responsible for increasing cardholder data controls to reduce credit card fraud. The Council suggests that organizations eliminate cardholder data where possible, as well as maintain communication with major financial organizations and credit card providers to reduce fraud or theft issues.

It also advises businesses to regularly monitor and take an inventory of their processes and IT assets to ensure they detect potential vulnerabilities as quickly as possible.

What Is the Need for POS Security?

POS security measures are crucial as data volumes increase exponentially alongside the growth in known and unknown attack vectors and security threats. The data held within POS systems is hugely valuable and could be highly damaging for organizations and their customers if it is lost or stolen.

Organizations that rely on POS systems must prioritize POS security to protect their sensitive customer data and prevent the breach of customer payment information. They must introduce measures that protect POS systems and safeguard customer transactions, and provide training for employees on the risks of POS security policies and incidents.