Qualys

CYBER SECURITY AND IMPORTANCE

WHAT IS CYBER SECURITY?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks typically aim to access, alter, or destroy sensitive information, extort money from users, or disrupt normal business processes. While some components of cyber security are designed to strike first, most of today's professionals focus more on determining the best way to defend all assets, from computers and smartphones to networks and databases, from attacks.

Cyber security has been used as a catch-all term in the media to describe the process of protection against every form of cybercrime, from identity theft to international digital weapons. These labels are valid, but they fail to capture the true nature of cyber security for those without a computer science degree or experience in the digital industry.

WHY IS CYBERSECURITY IMPORTANT?

In today's interconnected digital world, everyone benefits from advanced cyber defense programs. On an individual level, a cybersecurity attack can result in anything from identity theft to extortion attempts to the loss of important data such as family photos. Everyone relies on critical infrastructure such as power plants, hospitals, and financial service providers. Securing these and other organizations is essential to the functioning of our society. A single security breach can result in the exposure of millions of people's personal information. These security breaches have a strong financial impact on businesses and lead to the loss of customer trust. Therefore, cybersecurity is very important to protect businesses and individuals from spammers and cybercriminals.

TYPES OF CYBERSECURITY THREATS

Common cyber threats are:

- **Malware** such as ransomware, botnet software, RATs (remote access Trojans), rootkits and bootkits, spyware, Trojans, viruses and worms.
- **Backdoors**, which allow remote access. Formjacking, in which malicious code is inserted into online forms.
- **Cryptojacking**, in which illegal software is installed to mine cryptocurrencies.
- **DDoS (Distributed Denial of Service) attacks**, in which servers, systems, and networks are flooded with traffic to take them offline.
- **DNS (Domain Name System) poisoning attacks**, in which DNS is compromised to redirect traffic to malicious websites
- **Phishing** is the practice of sending fraudulent emails that resemble emails from reputable sources.
- **Social engineering** is a tactic that adversaries use to trick you into revealing sensitive information.

TYPES OF CYBER SECURITY?

Infrastructure Security

Infrastructure security is the practice of protecting critical systems and assets from physical and cyber threats. From the perspective of IT, this typically includes hardware and software resources such as end-user devices, data center resources, network systems, and cloud resources.

Network Security

Network security involves addressing vulnerabilities in your operating systems and network architecture, including servers and hosts, firewalls and wireless access points, and network protocols.

Cloud Security

Cloud security is concerned with securing data, applications, and infrastructure in the Cloud.

IoT (Internet of Things) Security

IoT security is about securing smart devices and networks connected to the IoT. IoT devices include things that connect to the Internet without human intervention, such as smart fire alarms, lights, thermostats, and other devices.

Application Security

Application security involves addressing vulnerabilities resulting from insecure development processes in designing, coding, and publishing software or a website.

THE CHALLENGES OF CYBER SECURITY

Cyber Security is becoming a severe issue for individuals, enterprises, and governments alike. In a world where everything is on the internet, from cute kitten videos and our travel diaries to our credit card information, ensuring that our data remains safe is one of the biggest challenges of Cyber Security. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people and attackers are becoming more innovative. Mitigating cybersecurity risks to your organization can be challenging. This is especially true if you have transitioned to telecommuting and have less control over employee behaviors and device security. An effective approach must encompass your entire IT infrastructure and be based on regular risk assessments.

BENEFITS OF CYBER SECURITY

The following are the benefits of implementing and maintaining cybersecurity:

- Cyberattacks and Data Breach Protection for Business.
- Data and network security are equally protected
- Unauthorized user access is prevented.
- Faster recovery is possible after a security breach.
- End-user and endpoint protection.
- Regulatory compliance.
- Continuity of operations.

HOW DO WI-FI HACKS HAPPEN, AND WHAT DOES IT MEAN TO YOU ?

SNIFFING

This involves a malicious actor using readily available software to intercept data being sent from, or to your device

Example Scenario

You are at a local coffee shop using free Wi-Fi to login to an email account that doesnt encrypt your login credentials.

A malicous actor is sitting in his car outside, using a free software to capture the information you submit. He is able to access your account information and potentially uses the same data to access your account, such as online banking or online shopping

SIDEJACKING

This attack involves sniffing data packets to steal session cookies and highjack user's session. These cookies can contain uncryted sensitive data, even if site is secure

Example Scenario

You are on your social networking site and suddenly your status is updated without you doing so.When you started that browser session and hacker was eavesdropping and hijacked your session. While she doesnt necessarily hace your password, she can impersonate you during your open session to access messages and send information to contacts

EVIL TWIN

This is a rogue Wi-Fi network that appears to be a legitimate network. When users unknowingly joins the rogue network the attacker can launch a man-in-the-middle attack, intercepting all data between you and the network

Example Scenario

You are the airport, waiting for your flight. You take advantage of the free Wi-Fi but there are multiple networks to join. You choose the one with the best connection un-aware that its a rogue Wi-Fi network created by a hacker. Once connected he installs malicious software and steals your sensitive data

MALVERTISING

ABOUT

- Malvertising (Malicious advertising) is the attack via online/web advertisements to spread malware. These ads spread malware through a legitimate website.
- These malware ads look authentic but once clicked upon they re-direct the user to a malicious website or install the malware in the user's device.

HOW DOES IT WORK?

- Malvertisements are distributed via the same methods as normal online advertisements. Infected graphic files are submitted to a legitimate advertisement network with hopes that the advertiser won't be able to differentiate between trustworthy ads and harmful ones.
- You can fall victim to malvertising by either clicking on an infected ad or even by visiting a website that is home to corrupted ads.

BEWARE IN ACTION

Nothing catches the eye like a stunning visual online advertising. The image stops a potential user in their middle of work, draws them in, and allows the user to get trapped in the cyber attack.

- Advertising of Flash games.
- Advertising of Free downloads/ software.
- Illegal streaming
- Advertising of Not safe for work content.
- Advertising of Online dating.
- Advertising of obscene content
- Popup claiming your device is infected.
- Advertising of free coupons/discounts.

HOW TO PROTECT YOURSELF

- Use an ad blocker plugin in your browser to block all ads while you're browsing. This way there won't be any uncenescessary ads.
- Avoid Clicking on too-good-to-be-true Google or Facebook/ social media ads.
- Ignore Web pop-ups that say software is out-of-date or prompting to install antivirus.
- As a general rule, you should resist clicking on ads, no matter how credible the site

DO'S

&

DONT'S

फ्रेंड रिक्वेस्ट स्वीकार करने से पहले, हमेशा उस व्यक्ति की प्रामाणिकता की जांच करें।

Always check the authenticity of the person before accepting friend requests online

ऐसी अज्ञात लिंक से बचें, जो ऑनलाइन एंटी-वायरस या एंटी-स्पाइवेयर सेवाएं प्रदान करती हैं।

Avoid unknown links that offer anti-virus or anti-spyware services online

मुफ्त में मिलने वाले सॉफ्टवेयर से सावधान रहें।

Beware of software that are available for free

सुनिश्चित करें कि आपकी ब्राउज़र सेटिंग्स में "ब्लॉक पॉपअप विंडो (block popup windows)" सक्षम है।

Ensure “block popup windows” is enabled in your browser settings

अनधिकृत सॉफ़्टवेयर स्थापित/इंस्टॉल न करें।

Do not install unauthorized software

किसी भी सॉफ्टवेयर को डाउनलोड करने के लिए भरोसेमंद और प्रामाणिक वेबसाइट का उपयोग करें।

Use trusted and authentic websites for downloading any software

ईमेल अटैचमेंट के माध्यम से प्राप्त किसी भी सॉफ्टवेयर को डाउनलोड करते समय सावधान रहें।

Be cautious while downloading any software received through email attachment

डाउनलोड के लिए आगे बढ़ने से पहले, संबंधित वेबसाइट के प्रमाणपत्र और प्रमाणपत्र जारी करने वाले की वैधता की जांच करें।

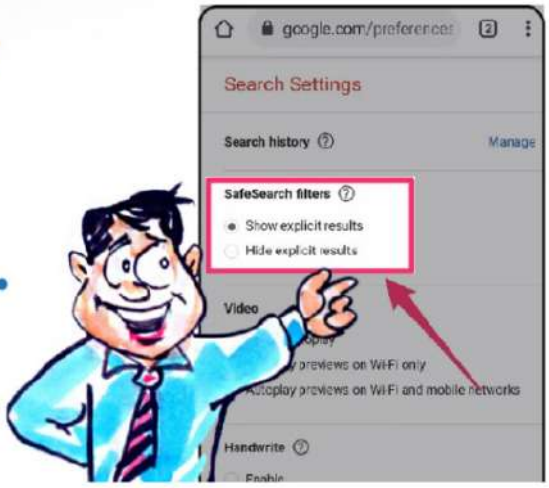
Check the validity of the certificate for a website and its issuer before proceeding with downloads

ब्लूटूथ के माध्यम से प्राप्त फाइलों से सावधान रहें।

Beware of the files received through Bluetooth

अपने ब्राउज़र सेटिंग्स में सुरक्षित खोज सक्रिय करें।

Activate Safe Search in your browser Settings



ऑनलाइन सेवाओं का उपयोग करते समय, महत्वपूर्ण व्यक्तिगत जानकारी पोस्ट करने से सावधान रहें।

Beware of posting critical personal information while accessing online services

स्वतः नवीनीकरण सक्षम होनेवाली अनचाही ऑनलाइन सेवाओं, पर नज़र रखें और अपनी सदस्यता रद्द (अनसब्सक्राइब) करना न भूलें।

Remember to track and unsubscribe unwanted online services which have auto renewals enabled

पाठ आधारित ईमेल में मुद्रा प्रतीकों का उपयोग करने से बचें, इसके बजाय स्पैम फ़िल्टर से बचने के लिए तीन-अक्षर वाले मुद्रा संकेतक जैसे (यू एस डी, आई एन आर) का उपयोग करें।

Avoid using currency symbols in text based emails, instead use three-letter currency indicators like (USD, INR) to avoid spam filters

एन्क्रिप्शन के लिए एक्सेस पॉइंट द्वारा समर्थित अधिकतम कुंजी आकार को हमेशा प्राथमिकता दें।

Always prefer the maximum key size supported for encryption by access point

ईमेल में संवेदनशील डेटा भेजने से बचें ।

Avoid sending sensitive data in emails

लॉटरी वाली ई-मेल का कभी भी जवाब न दें।

Never reply to lottery e-mails

मजबूत पासवर्ड का प्रयोग करें और उसे कभी किसी के साथ साझा न करें।

Use strong passwords and never share them

विभिन्न ऑनलाइन सेवाओं के लिए अलग-अलग पासवर्ड का उपयोग सुनिश्चित करें।

Ensure using different passwords for different online services

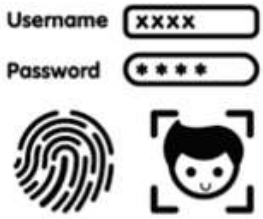
Secure Password Practices

> Your password is your first line of defense in Cyber Security .

1. Create strong password

- 08 to 10 characters,
- 2 Uppercase characters
- 1 number
- 1 special character.

Just this basically can make a password strong and complex, but this should not be common like PassworD@123



2. Avoid easy guess

Never use personal information (your name, children's name, date of birth, pet's name) that someone might already know or easily obtain. Avoid common dictionary words for creating a password.

3. Use a password managers

Password managers as a means of practicing high level of security and to help keep their sanity. With password managers, you only need remember one password as a password manager stores password for you.

4. Use different passwords for different accounts

It can be tempting to use the same password for every account, however this makes it easier for hackers to break into a multitude of accounts. Diversify your passwords by using a different passwords for every account.

5. Secure your mobile phone

With the growing use of mobile phones to conduct business, or access company sensitive information are becoming a major cause of concern in the security community. Securing your phones with a strong password or use fingerprint.

6. Replace passwords regularly

It can also be tempting to keep the same old passwords for years. or reuse as a new passwords. However, changing passwords regularly is a good password practices.

7. Change password when employer leaves company

Do not let former employees hack or gain unauthorized access into business accounts. By making it common practice to change passwords when an employee leaves the company.

8. Do not write, store and share your password for any reason

Password must not be inserted into email message or must not be share in any other form of electronic communication. Do not write password down and store them anywhere in your office.

Any employee found to have violated this guidelines may be subjected to disciplinary action.