Cyber Security Online

Cyber Threat: Your Personal Data is in Danger

One common problem when you are online is a "data breach". Imagine if your private information leaked out. That is similar to what a data breach is online.

A data breach happens when sensitive or personal information is accessed, exposed or stolen without authorization.

In online shopping, it can include names, addresses, payment details, or what you bought.

Cybercriminals want this information.

Data breaches can lead to identity theft and problems for online stores. It is a serious issue for everyone.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Cyber Security Online

Online Threats

Online threats are potential dangers that can compromise the security of our devices and data when we are online. Some common online threats include:

Spyware

Phishing

Spoofing

Malware

Ransomware

… and more.

They can lead to unauthorized access, data theft, and system damage.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Cyber Security Online

Cyber Threat:
Spyware - The Silent Thief

A threat to watch out for is "spyware". It is sneaky and hides on your devices.

Spyware is a type of malware that secretly monitors activity on a device.

It can collect information such as browsing history, passwords and financial data.

Some types can also record keystrokes, capture your screen or access other device functions.

Cybercriminals use this information to steal money or identity.

Spyware is a silent danger. Protect yourself by being careful with downloads and using reputable security software.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Cyber Security Online

Cyber Threat:
Phishing - Fake and Tricky Messages

Phishing is a cyberattack where cybercriminals pretend to be a trustworthy person or organization to steal your personal information.



How They Lure You In:

Phishing Emails: These emails often create a sense of urgency and use familiar logos and names to pressure you into clicking on links or revealing personal details.

Smishing & Vishing: Similar scams happen through text messages (smishing) and phone calls (vishing). They use urgency or intimidation tactics to trick you.

Fake Websites: Cybercriminals create websites that look real, stealing your login information when you try to log in.

© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Cyber Security Online

Cyber Threat:
Phishing - Fake and Tricky Messages

Red Flags to Watch Out For:

Urgency: Messages that pressure you to act immediately.

Unexpected Requests: Requests for passwords, payment or personal information.

Suspicious Sender: The email address or phone number does not match who the sender claims to be.

Suspicious Links or Attachments: Unexpected links, shortened URLs or files.

Unusual Language: Poor grammar or spelling can still be a warning sign, although modern phishing messages may look very professional.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Cyber Security Online

Cyber Threat:
Spoofing - Disguises Online

"Spoofing" is when attackers disguise information so that it appears to come from a trusted source.

Spoofing is a cyber deception tactic used to trick people or systems. It is like wearing a costume to look familiar. Attackers can spoof:

Email Addresses: Emails might appear to come from your bank or a familiar company, urging you to click a link or download an attachment containing malware.

Phone Numbers: You might receive calls that seem to be from your credit card company or tech support, attempting to steal your personal details.

IP Addresses: Attackers can manipulate IP information to appear as if they are coming from a trusted location.

Be careful! Do not trust online information just because it looks familiar. Always verify important requests through official channels.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Cyber Security Online

Cyber Threat:
Spoofing - Disguises Online



Shielding Yourself from Spoofing:

Scrutinize Sender Information: Do not trust email addresses or phone numbers at face value. Verify them through official channels.

Beware of Urgent Requests: Legitimate companies rarely pressure you for immediate action. Be cautious of emails or calls demanding swift action.

Verify Links Before Clicking: Do not click on links in emails or texts. Manually type the legitimate website address into your browser.

Verify Important Requests: If a message or call asks for money, passwords or sensitive information, contact the organization using a known official number or website.

Strong Passwords & MFA: Use unique passwords and enable Multi-Factor Authentication (MFA) for added security on your accounts.

By being alert and following these steps, you can make it harder for spoofers to deceive you.

© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Cyber Security Online

Cyber Threat:
Malware - Harmful Software Dangers

Malware stands for "malicious software."

Malware is software designed to damage systems, steal data, disrupt operations or gain unauthorized access. Cybercriminals use malware to achieve various malicious goals:

Stealing Information: Malware can steal sensitive data like passwords, credit card numbers, or personal files.

Disrupting Operations: Malware can crash your system, corrupt files, or prevent you from accessing your computer.

Spreading Further: Malware can replicate itself and infect other devices on your network.

Taking Control: In extreme cases, malware can give attackers remote access to your computer, allowing them to control it.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Cyber Security Online

Cyber Threat:
Malware - Harmful Software Dangers



Shielding Yourself from Malware:

Antivirus and Anti-Malware Software: Install and maintain reputable antivirus and anti-malware software that scans for and removes malware threats.

Be Wary of Downloads: Only download software from trusted sources. Avoid clicking on suspicious links or opening attachments from unknown senders.

Keep Software Updated: Outdated software can have security vulnerabilities. Regularly update your operating system, web browser, and other applications.

Passwords, Passkeys & MFA: Use unique passwords with a password manager, enable MFA, and use passkeys where available.

Be Cautious of Free Offers: If something seems too good to be true online, it probably is. Avoid clicking on pop-up ads or downloading free software from unreliable sources.

© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Cyber Security Online

Cyber Threat:
Ransomware - Data Held Hostage

"Ransomware" is a particularly nasty type of malware. It locks your files and demands money to unlock them.

Ransomware encrypts your files, making them unusable.

Cybercriminals demand a "ransom" payment, often in cryptocurrency.

Without a working backup or recovery method, you may lose access to your data.

Ransomware attacks can severely disrupt logistics and online shopping.

Do not pay the ransom. Why? (Discussion)

Ransomware can be devastating. Back up your data regularly. Payment does not guarantee recovery, supports criminal activity, and can sometimes create legal problems. Report attacks to the authorities.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Cyber Security Online

Cyber Threat:
Ransomware - Data Held Hostage

Shielding Yourself from Ransomware:

Regular Backups: Keep recent backups of important files, including at least one copy that ransomware cannot easily access or modify.

Software Updates: Keep your operating system, applications, and security software up-to-date to patch vulnerabilities that attackers exploit.

Beware of Attachments & Links: Exercise caution with email attachments and links, especially from unknown senders. Do not click on suspicious links or download unsolicited files.

Anti-Malware Software: Use a reputable anti-malware program that can detect and potentially block ransomware attacks.

Do Not Pay the Ransom: Paying does not guarantee recovery and can encourage further attacks. Report the incident and seek professional or law-enforcement guidance.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Cyber Security Online

Other Online Threats
And More to Be Aware Of

Besides these main threats, there are many other online dangers to be aware of in online shopping.

...and more: The world of cyber threats is always changing.

New types of malware and attacks appear all the time.

Account takeover and credential theft are also common risks.

Being vigilant and cautious is key to online safety.

Always be aware that online threats are evolving. Stay updated on cybersecurity news and best practices to protect yourself.

Keep up to date by regularly visiting sites like StaySafeOnline.org and GetSafeOnline.org.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Cyber Security Online

Other Ways to Stay Safe Online

In addition to the tools we discussed, there are other security steps too! It is like having many locks on your door, not just one.

Encryption protects your data by making it unreadable without the right key.

Use 2FA or MFA whenever possible.

Use long, unique passwords, a password manager or passkeys where available.

Cybersecurity training helps you spot threats.

Updates and regular checks keep systems more secure.

Using different security methods together is the best way to stay safe online. It is like a team effort!



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com