Open Access Research Journal of
Science and Technology
Journals home page: https://oarjst.com/
ISSN: 2782-9960 (Online)

OARJ OPEN ACCESS RESEARCH JOURNALS

(Review Article)

Check for updates

Cybersecurity and personal privacy: Protecting yourself in the digital age

Ahmed Al Zaidy *

Information Technology Programs, Florida State College at Jacksonville, Jacksonville, Florida, USA.

Open Access Research Journal of Science and Technology, 2024, 12(01), 131–135

Publication history: Received on 27 August 2024; revised on 11 October 2024; accepted on 14 October 2024

Article DOI: https://doi.org/10.53022/oarjst.2024.12.1.0122

Abstract

The internet has revolutionized communication, work, and life, offering unprecedented opportunities and conveniences. However, as our dependence on the digital world grows, so do the risks to our personal information, privacy, and security. Cyberattacks, online harassment, and cyberstalking are no longer rare occurrences—they have become everyday threats that anyone can face. Understanding and implementing robust cybersecurity measures is essential for protecting yourself in this increasingly connected world. This article explores effective ways to safeguard against cyberattacks, respond to online harassment, prevent cyberstalking, and remove your personal information from websites that share it without your consent.

Keywords: Cybersecurity; Online privacy; Cyberattacks; Online harassment; Data protection

1. Introduction

Cyberattacks have become a constant threat in today's interconnected world, targeting individuals, businesses, and governments. Cybercriminals deploy tactics, such as phishing scams, ransomware, and identity theft, to gain unauthorized access to sensitive information, causing financial loss, data breaches, and reputational damage. However, you can significantly reduce the risk of falling victim to such attacks by adopting proactive cybersecurity measures [1],[2] and [3].

By implementing strong passwords, enabling two-factor authentication, regularly updating your software, and exercising caution with suspicious links, attachments, and insecure Wi-Fi networks, you can fortify your defenses against cyberattacks. Additionally, backing up important data and staying informed about the latest threats is essential to protect your digital life [2].

This guide covers key strategies, including the importance of password security, software updates, and network protection, that can help you stay ahead of cybercriminals and safeguard your personal and professional information from cyberattacks.

2. Safeguarding Against Cyberattacks

Cyberattacks can take many forms—phishing scams, ransomware, identity theft, and more. These attacks can result in stolen personal information, financial loss, and even damage to your reputation. Fortunately, there are several steps you can take to minimize the risk of falling victim to these cybercrimes [1], [3] and [6].

2.1. Strong Passwords and Two-Factor Authentication

Passwords are the first line of defense for your online accounts, yet many people still use weak or easily guessed passwords like "password123" or their birthdate. Create complex passwords that combine uppercase and lowercase

* Corresponding author: Ahmed Al Zaidy

letters, numbers, and symbols to secure your accounts truly. Avoid using personal information, such as your name or phone number, and make sure each account has a unique password [2] and [4].

A password manager can help generate and store these passwords securely. These tools create strong, randomized passwords and ensure you don't have to remember each one. Furthermore, enabling two-factor authentication (2FA) on your accounts adds a security layer. With 2FA, even if a hacker obtains your password, they'll need a second form of identification (such as a code sent to your phone) to access your account. This makes unauthorized access far more difficult [2].

2.2. Regular Software Updates

Cybercriminals often exploit vulnerabilities in outdated software. When developers discover these security flaws, they release updates to patch them. Unfortunately, many people delay or ignore software updates, leaving their devices vulnerable to attacks. To protect yourself, set your devices to install updates automatically whenever new versions are released [2].

These updates aren't limited to your operating system—applications like web browsers, antivirus software, and even mobile apps also need regular updates. Keeping all of your software up to date ensures that known vulnerabilities are fixed, reducing your exposure to potential threats.

2.3. Avoid Suspicious Links and Attachments

Phishing attacks are among the most common ways hackers access personal information. These scams often involve emails or messages that appear to come from legitimate sources, such as your bank or a trusted company, but contain malicious links or attachments designed to steal your data.

To avoid these scams, always be cautious when opening unsolicited emails, especially if they ask for personal information or prompt you to click a link. Hover over the link to check the URL; if it looks suspicious or unfamiliar, don't click on it. Contact the sender directly to verify the message's authenticity when in doubt.

2.4. Secure Your Wi-Fi

Your Wi-Fi network can be a target for cybercriminals, especially if it's not properly secured. Ensure that your home Wi-Fi is password-protected and that you're using the latest encryption method, such as WPA3, which is more secure than older protocols like WEP or WPA2. A weak or unsecured Wi-Fi network can allow hackers to access your devices, steal sensitive information, or install malware.

When using public Wi-Fi networks, such as those in coffee shops or airports, avoid conducting sensitive activities like online banking or shopping unless you're using a Virtual Private Network (VPN). A VPN encrypts your internet connection, making it harder for attackers to intercept your data.

This table shows the differences between common Wi-Fi encryption methods and highlights the importance of using modern standards like WPA3.

Table 1 Wi-Fi Security Protocols

Security Protocol	Description	Security Level	Recommended?
WEP	Early encryption, easily cracked	Low	No
WPA	Improved over WEP but still weak	Medium	No
WPA2	Stronger, common in most networks	High	Yes, but outdated
WPA3	Latest encryption standard	Very High	Yes

2.5. Backup Your Data

In the event of a cyberattack—especially ransomware—your data may be held hostage, or your files could be corrupted or destroyed. Regularly backing up your important files to an external hard drive or a secure cloud service ensures you have copies of your data in an emergency. Set up automatic backups for maximum convenience and protection and periodically test them to ensure they function properly.

3. Dealing with Online Harassment

Online harassment has become a widespread issue, ranging from mean-spirited trolling to severe cases of stalking and threats. Unfortunately, online anonymity can encourage individuals to engage in behavior they wouldn't consider in person. If you're facing online harassment, there are several steps you can take to protect yourself and respond effectively.

3.1. Control Your Privacy Settings

Many social media platforms offer detailed privacy settings that allow you to control who can see your posts and personal information. Regularly review and update these settings to ensure that only trusted individuals can view your content. Limiting who can see your posts reduces the chances of becoming a target for harassers.

Be mindful of the information you share online, especially regarding your location, daily routines, or personal life. The more details you make public, the easier it is for someone to use that information against you.

3.2. Block and Report Offenders

Most social media platforms and online forums provide tools to block users and report inappropriate behavior. If you're being harassed, use these features to prevent further contact with the individual. Blocking the harasser will stop them from sending you messages or interacting with your posts, while reporting them can lead to further action by the platform, such as suspending or banning their account.

In addition to blocking and reporting, keep a record of the harassment. Take screenshots of any offensive or threatening messages, as this documentation may be useful if you decide to involve law enforcement or pursue legal action.

3.3. Avoid Engagement

Engaging with online harassers often exacerbates the situation. Trolls and bullies thrive on attention and will continue their behavior if they see that it elicits a response. The best course of action is often to ignore them entirely. By not responding, you deprive them of the satisfaction of knowing they've affected you.

If the harassment escalates or becomes threatening, consider seeking support from a trusted friend, family member, or mental health professional. Dealing with harassment can be emotionally taxing, and having a support system in place can make a significant difference.

3.4. Seek Legal Help

In cases of severe or persistent harassment, legal action may be necessary. Many countries have laws that protect individuals from online harassment, and depending on the severity of the case, law enforcement may be able to intervene. If you feel threatened or unsafe, don't hesitate to contact local authorities and seek legal advice.

4. Preventing and Responding to Cyberstalking

Cyberstalking is a form of harassment that can have devastating effects on victims. It involves persistent, unwanted contact or monitoring, often escalating to threats or actual harm. While anyone can become a victim of cyberstalking, there are ways to reduce your risk and protect yourself [5].

4.1. Minimize Your Digital Footprint

Cyberstalkers often rely on publicly available information to track their victims. Minimizing the amount of personal information you share online makes it more difficult for them to gather details about your life. Avoid sharing sensitive information like your home address, phone number, or place of work, especially on social media [5].

Regularly search your name on search engines to see what information is publicly available. If you find sensitive data, take steps to have it removed from websites or data broker services (explained further below).

4.2. Secure Social Media Accounts

Keeping your social media profiles private is one of the best ways to protect yourself from cyberstalkers. Set your profiles to "private" or "friends only" so approved connections can see your posts and personal information. Be cautious about accepting friends or following requests from people you don't know in real life [5].

Avoid sharing your location in real time, especially through location tags or check-ins. Stalkers can use this information to track your movements and learn your routines, risking your physical safety.

4.3. Use Encrypted Communication

If you suspect you're being cyberstalked, use encrypted messaging apps such as Signal or WhatsApp for sensitive conversations. These apps use end-to-end encryption, which means only the intended recipient can read your messages. This prevents unauthorized individuals, including cyberstalkers, from intercepting your communications [2].

Additionally, consider changing your phone number or email address if a stalker contacts you through those channels. Creating new, private accounts for communication can help break the cycle of unwanted contact.

4.4. Monitor Your Devices

Cyberstalkers may use spyware to track your online activities or monitor your devices remotely. Be vigilant about unusual signs on your devices, such as sudden battery drain, unexplained data usage, or new apps you didn't install. Antivirus software scans your devices for spyware or malware and removes suspicious applications [5].

In extreme cases, you may want to consider performing a factory reset on your device to remove any malicious software entirely. If the cyberstalker has compromised your device, starting fresh can help you regain control of your digital privacy.

5. Opting Out of Data Brokers and Public Information Sites

One of the most alarming aspects of modern internet use is the prevalence of websites that collect and publish personal information without your consent. These data broker sites aggregate information from public records, social media, and other sources, making it easy for anyone—including potential stalkers or harassers—to find your home address, phone number, or other personal details. Fortunately, many of these sites offer opt-out processes to remove your information.

5.1. Identify Data Broker Sites

Start by searching for your name on major search engines and your city or state. This will likely lead you to data broker sites like Whitepages, Spokeo, BeenVerified, and others that may have published your personal information. Keep a list of the sites where your data appears.

These sites often compile information from public records, such as property ownership, voter registration, or professional licenses. While they claim to offer useful services for locating people or conducting background checks, they also pose a serious risk to your privacy.

5.2. Submit Opt-Out Requests

Each data broker website typically has an opt-out process detailed in their privacy policy or a "Do Not Sell My Info" section. This process usually involves submitting a request to have your personal information removed, which may require you to provide proof of identity, such as a scanned copy of your driver's license. While this step can be cumbersome, it's crucial for protecting your privacy.

After submitting your opt-out request, monitor the site to ensure your information has been removed. Remember that the removal process can take several weeks, and in some cases, your data may reappear over time.

5.3. Use Automated Services

If manually opting out of each data broker site feels overwhelming, consider using automated services like DeleteMe or Privacy Bee. These services submit opt-out requests on your behalf to multiple data broker sites, saving you time and effort. While there is usually a subscription fee, these services can provide peace of mind, especially if you're concerned about your personal information being widely available.

5.4. Check Regularly

Even after opting out, checking whether your information has been re-listed periodically is important. Data brokers continuously update their databases, and your details may be re-added from public records or other sources. Conduct regular searches for your name and repeat the opt-out process if necessary [6].

The table below lists popular data broker sites and summarizes how users can remove their personal information.

Table 2 Popular Data Broker

Data Broker	Opt-Out Process	Processing Time	Difficulty
Whitepages	Submit an online request, verify the identity	1-2 weeks	Moderate
Spokeo	Email request, verify identity	2-4 weeks	Moderate
BeenVerified	Online form, verify identity	One week	Easy
MyLife	Email or mail, verify identity	1-2 weeks	Moderate

6. Conclusion

In today's digital world, cybersecurity is no longer optional—it's essential. By adopting best practices such as creating strong passwords, securing your Wi-Fi, and keeping your software up to date, you can significantly reduce the risk of cyberattacks. If you're facing online harassment or cyberstalking, protecting your privacy and engaging with law enforcement can help you regain control. Finally, taking the time to remove your personal information from data broker websites is crucial for protecting your privacy in the long term. Being proactive and vigilant can safeguard your personal information and online safety in the digital age.

References

[1] Cybersecurity and Infrastructure Security Agency, Cybersecurity, CISA.gov. [Online]. Available: https://www.cisa.gov/cybersecurity. [Accessed: 26-Sep-2024].

[2] National Institute of Standards and Technology, Cybersecurity Framework, NIST.gov. [Online]. Available: https://www.nist.gov/cyberframework. [Accessed: 26-Sep-2024].

[3] Federal Trade Commission, Privacy, identity & online security, FTC.gov. [Online]. Available: https://www.consumer.ftc.gov/topics/privacy-identity-online-security. [Accessed: 26-Sep-2024].

[4] Electronic Frontier Foundation, Surveillance self-defense, EFF.org. [Online]. Available: https://ssd.eff.org. [Accessed: 26-Sep-2024].

[5] Pew Research Center, Online harassment and cyberstalking, PewResearch.org. [Online]. Available: https://www.pewresearch.org/fact-tank/2021/01/13/online-harassment-2021/. [Accessed: 26-Sep-2024].

[6] Identity Theft Resource Center, Protect your personal information, IDTheftCenter.org. [Online]. Available: https://www.idtheftcenter.org. [Accessed: 26-Sep-2024].