ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

# Cybersecurity in Day-to-Day Life : A Technical Perspective

**Bhanuprakash Madupati**

Cision, NC, USA

**ABSTRACT**

Cybersecurity has become one of the most important elements of our daily lives, both for individual and business purposes, as we are connected virtually more than ever. With threats of all kinds, from those targeting personal mobile devices to phishing attacks and ransomware, the importance of thorough cybersecurity practices cannot be overstated. In this paper, we provide hands-on practical insights into how one might apply cybersecurity practices to what is soon to be (if not already) everyday activities. The paper focuses on common cyber threats, such as phishing or ransomware, and includes practical technical solutions to reduce the risks resulting from these attacks. Multiple reports on this problem have been improved in the paper by proposing multi-factor authentication, encryption protocols, permanent propagation patches, and user education as basic elements of a proactive cybersecurity strategy. Learning and applying these safety measures is critical in protecting personal details and preserving privacy in a world where people continually access digital technology daily.

***Corresponding author**

Bhanuprakash Madupati, Cision, NC, USA.

**Received:** January 03, 2022; **Accepted:** January 10, 2022, **Published:** January 17, 2022

**Keywords:** Cybersecurity, Wi-Fi Security, Mobile Devices, Phishing, Ransomware, IOT Security

## Introduction

- **Cybersecurity Fit in Our Day-To-Day Lives**

  Technology touches nearly every facet of our lives in today's fast-paced, interconnected environment, from communication and entertainment to banking and healthcare. This internet-led transformation incremented a new threat landscape that became a significant new threat to our digital world in the form of cyberattacks that are increasing in magnitude and complexity. Each internet-enabled device—a mobile handset, laptop, or smart home gadget — represents an opportunity for bad actors who want to steal proprietary data, disrupt services, or hold users at ransom. Therefore, it is no longer an issue of only organizations and governments worrying about cybersecurity.

  Simple tasks, such as checking emails or browsing the net with public Wi-Fi, purchasing on the web, or controlling IoT devices, put people at intentional risk of cybersecurity. Given the ubiquity of technology in our personal and professional lives, there is an urgent call for improved security solutions to shield against data breaches. If such precautions are not taken, this poses difficult repercussions like a breach of identity, loss of money, and unauthorised access to personal information.

- **Objective of the Paper**

  This paper offers a technical perspective on day-to-day follow-ups that are helpful in cybersecurity. The course also discusses common cyber threats like phishing, ransomware, mobile device vulnerabilities, and insecure Wi-Fi networks. It describes technical measures that organisations can undertake to combat these threats. The paper will also discuss how technologies like Multi-Factor Authentication (MFA), encryption, and regular security updates can be deployed to protect personal and home digital systems. The study underlines the vital role that education and awareness play in finding a way for people to manage the ever-changing cybersecurity world.

## Common Cybersecurity Threats

With our digital footprint expanding daily, we are all prone to several cybersecurity threats. The threat landscape includes everything from Vegas-quality phishing schemes to mobile devices, WiFi networks, and many other entry points. The following section details the prime cybersecurity threats individuals face and concludes their effects.

- **Phishing Attacks**

  Among the various cyber-attacks common today, phishing is one of the foremost threats individuals encounter. Phishing emails or messages are disguised as being from a credible source, with the idea of getting users to share sensitive information such as email credentials, credit card digits, or social security numbers. AA's recent research paper found that phishing is still one of the most efficient ways cybercriminals steal user data [1].

- **Phishing:** Phishing attacks are among the most dangerous forms of cybercrime, mainly because they often dodge conventional security measures such as firewalls and antivirus software. Attackers may use convincing language and legitimate-looking websites to fool users, which complicates differentiating a real request for information from a fake one. In an era where email and messaging platforms have become the primary communication channels for many, the overwhelming increase in Phishing attacks puts more people at risk.

**Table 1: Common Indicators of Phishing Attacks**

| • Indicator | • Description |
|---|---|
| • Suspicious Email Address | • The sender's email address doesn't match the official domain. |
| • Generic Greetings | • Messages start with "Dear Customer" instead of using your name. |
| • Urgent Language | • Language that pressures you to act immediately |
| • Mismatched Links | • Hovering over a link shows a different URL than expected. |
| • Requests for Sensitive Information | • Asking for passwords or payment details over email |

**• Ransomware**

Ransomware is a further severe danger. It attacks people and groups by encrypting facts for a ransom. The growing prevalence of anonymous payment systems like cryptocurrency has been attributed to the uptick in ransomware attacks. In particular, ransomware has caused widespread chaos by targeting hospitals, municipalities, and personal devices.

A typical ransomware attack lifecycle often starts with an initial malicious download, frequently through phishing emails. After infection, the victim's files are encrypted, and a ransom is demanded to obtain the decryption keys. Nevertheless, paying the ransom does not mean your data will be returned [2].


**Figure 1:** The Ransomware Lifecycle

**• Vulnerability of Mobile Devices**

Although mobile devices are so important to our daily lives, they are still at high risk for cyber threats. Mobile malware can navigate through these devices to access personal and sensitive data like financial information, location data, and communication logs. Another major flaw is in the app's permissions, which are asked more than they should have been. When granted to a third-party application, most of these permissions open more gates to user data, increasing the possibility of data leaks [3].

In addition, users can use these devices on unsecured public Wi-Fi networks, leading to more cybersecurity dangers. This is because an attacker can attack communications over these networks, which could result in the security of your data [4].

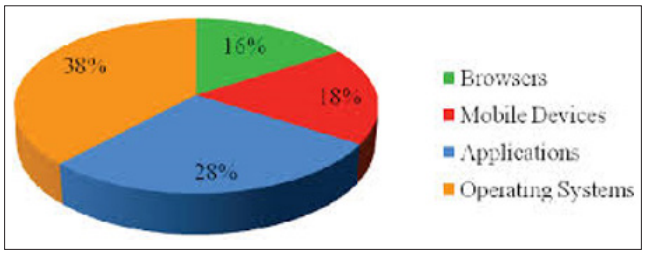


**Figure 2:** Breakdown of Mobile Device Vulnerabilities

**• Wi-Fi and Network Security**

Given their inherent vulnerabilities, Wi-Fi networks—particularly public ones—are prime hunting grounds for cyber criminals. Wireless communications are easily intercepted, as WEP and WPA encryption protocols proved not innocent of snoopers. WPA2 is much more secure but also plagued with flaws, as seen with the KRACK attack.

These stronger layers of encryption found in the WPA2 and WPA3 protocols are not without mention that many home and public networks still rely on less secure protocols. Thus, moving to WPA3 would be great for helping you secure from today's and tomorrow's cyber threats. Since these wireless networks are included in everyday communication and internet access, securing them will keep personal data safe.

**Table 2: Comparison of Wi-Fi Security Protocols**

| • Security Protocol | • Encryption Method | • Vulnerabilities |
|---|---|---|
| • WEB | • RC4 | • Easily cracked, outdated |
| • WPA | • TKIP | • Weak encryption, vulnerable to attacks |
| • WPA2 | • CCMP (AES) | • Stronger security, but WPA2 is susceptible to KRACK attacks |
| • WPA3 | • GCMP-256 (AES) | • Enhanced security, robust against modern attacks |

**• IoT Devices & Smart Homes**

Smart homes are becoming more common, and the IoT (Internet of Things) devices they hold ensure that security threats to these smart homes evolve. For example, few internet-connected devices, such as smart thermostats, security cameras, and voice assistants, come with strong security protections.

One of the most famous examples is the Mirai botnet, which was involved in a massive DDoS attack in 2016 that utilized thousands of compromised IoT devices. Cybersecurity experts Jumping Bean said the attack showcased how poor-quality IoT devices could be used to compromise wide networks.

**Cybersecurity: Technical Actions**

Many technical solutions are being deployed to help people protect themselves from the ever-growing range of security threats they experience daily. These solutions include using strong wireless network encryption technologies for homes and strong authentication methods to defendg against phishing attacks and ransomware. Best Technical Solutions: The tutorial section discusses what type of technical solutions are most effective for improving personal cybersecurity.

**• Securing Wireless Networks**

It is important to secure Wi-Fi networks, as data is no longer transmitted over the Internet but within home environments, and weak encryption protocols, including Wired Equivalent Privacy (WEP) or Wireless Protected Access (WPA), may be used. The change from old-school encryption protocols to new ones like WPA2 and WPA3 is more protective against cyber adversaries. WPA3 largely enhances encryption by enforcing GCMP-256 and introduces forward secrecy, meaning all traffic exchanged through the wireless network will not be decryptable even when a key is compromised [5].

Some home networks still employ WPA2, a stronger security standard compared to previous generations of wireless encryption, but it is nonetheless susceptible to the recently exposed KRACK (Key Reinstallation Attack) exploit. This vulnerability can be mitigated by upgrading to WPA3, which should add extra security layers to wireless communication at home and in public (in theory).


**Figure 3:** Wi-Fi Security Protocol Evolution

**• Multi-Factor Authentication (MFA)**

When Users Join In On Exposing Themselves…by Jessica Bromall SparkPost BlogPolicy & Compliance1 min readWhat else can the good and fine folks of Policy do regarding data breaches? MFA is a blend of two or more verification methods, including passwords, biometrics, and tokens, to validate the actual user. When properly implemented, MFA systems can greatly reduce unauthorized access, particularly when password-only protection is inadequate.

One such application is Cyber-Physical Systems (CPS), widely used in industrial and domestic settings. These systems also benefit from MFA in addition to other security layers. MFA ensures system access security and, when integrated with data analytics, can assist in identifying irregular behaviour, such as a possible sweat spot, which can lead to stolen information.

**Table 3: Common MFA Methods and their Benefits**

| • Authentication Method | • Description | • Benefit |
|---|---|---|
| • Password | • Something the user knows | • Basic security, but easily compromised |
| • Biometric (fingerprint, face) | • Something the user is | • Difficult to replicate |
| • Token (hardware or app) | • Something the user has | • Adds physical security layer |
| • Randomized Factors | • Combination of unpredictable factors | • Reduces predictability for attackers |

**• Anti-Phishing Measures**

One of the most effective ways criminals can obtain personal information is through phishing attacks. It sounds bleak and fishy, and despite all these technical drawbacks, both technical measures and user education can reduce the threat of phishing. It is one of the phishing training systems by which users are aware of phishing attacks, like in phishing sandboxes, and an approach to simulate a particular email scam attack is called cyber threat emulation. These systems send out simulated phishing emails to users and monitor results, an effective way to train your employees on what to watch for in real-world phishing attacks.

In addition to training, technical solutions such as email filtering, domain-based message authentication (DMARC), and installing system updates can also be used. These measures can greatly reduce the spam messages that make it into user inboxes, and browser alerts can block access to malicious websites.

**• Protecting Mobile Devices**

Since mobile devices are becoming increasingly important in daily activities, keeping them free from malware, data leaks, and unauthorised access is necessary. Recently, researchers have explored the idea of transient authentication and created solutions that provide continuous and context-aware checking without hindering user exercise. Transient: For example, that could mean authenticating a user based on their historical usages, like geo-location, device interaction, or behaviour patterns.

In addition, several preventive measures, like app permission management and timely device updates, minimise mobile devices' vulnerability. Over-permission apps are designed to collect personal data. Limiting app permissions to protect only what is absolutely necessary and not using public Wi-Fi will greatly minimise the threat of unauthorised access.


**Figure 4:** Key Steps to Protect Mobile Devices

**• Ransomware Prevention**

Ransomware attack prevention requires a mix of preemptive preparation and reactive incident response. The Best Defense is a Good Backup: First, regular backups of sensitive data are one of the most effective defenses against ransomware. If people have an offsite or cloud-based backup system, they might be able to revert their files to normal to avoid paying the ransom in case of an attack.

In addition, using antivirus software and updating the security system can prevent ransomware attacks. Security patches close doors to known security holes that the ransomware utilises, and

antivirus software recognises and isolates corrupt data before it can be encrypted on the victim's systems.

## Case Studies and Practical Examples

Examples of practical implementation in real life provide readers with case studies and scenarios from live situations, which are taken apart and illustrated in detail. These examples indicate what doesn't work regarding security, including phishing training, IoT practices, and Wi-Fi network protection.

### • Phishing Attack Prevention

Phishing attacks are some of today's most prevalent cyber threats directed at individual users and all types of enterprises. One successful way to fight phishing is with end-user training and awareness programs that help people identify possible phishing attempts. One study provides an example of an anti-phishing training system, which could be a part of the practical side that would help raise awareness among users and teach them what phishers use phishing techniques.

This system will use Tactics, Techniques and Procedures (TTPs) to simulate phishing attacks that real adversaries use. The intent is to make it harder for users to recognise malspam and click on malicious links. Without question, this type of training greatly decreases the probability of a user being successfully scammed by a phishing email over time as it improves their capacity to recognise malicious emails. Those who have implemented this method of practising have noticed a dramatic reduction in the number of click-throughs through potential phishing attempts by their employees [5].

This real-life scenario shows how technical intervention and regular user training can help mitigate the risks associated with phishing attacks in daily life.

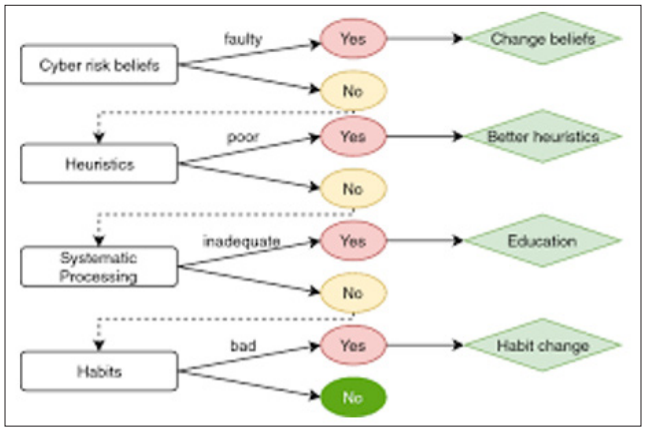


**Figure 3:** Anti-Phishing Training System Workflow

### • Hardening the IoT of a Smart Home

Since IoT devices are now prevalent in homes, it is essential to secure them better so as not to risk privacy breach breaches and to have unauthorised access to home networks. This is illustrated by the Mirai botnet case, which showed that many IoT devices are vulnerable due to find-the-password security and easy-to-guess default passwords shipped with the devices [4].

A couple of measures for this would be the enforcement of multi-factor authentication (MFA) and the establishment of software updates scheduled for IoT devices. A recent study has revealed that pairing MFA with strong data analytics greatly improved security within IoT systems — providing a better mechanism to keep unauthorised users out and quickly identify erratic behaviour [6]. This use case proves that effective smart home security needs to begin with individual responsibility (e.g., stop using default passwords) and rely on technical protections (such as MFA, automated threat response >/detection/anomaly detection).

By adopting these security practices, homeowners can greatly decrease the chance that their devices will be co-opted into large-scale attacks–such as the incident with the Mirai botnet [2].

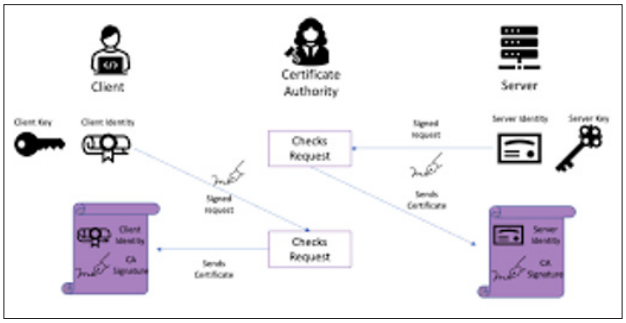


**Figure 4:** Multi-Factor Authentication in IoT Devices

### • Wi-Fi Security in Public Locations

Public Wi-Fi is super convenient, but it can also be treacherous. Public Wi-Fi networks are generally unsecured, so hackers can intercept data travelling over them more easily. One study comparing the efficacy and security of different Wi-Fi security protocols showed that weak legacy protocols like WEP and WPA are easily attackable, leaving encryption and integrity poorly secured.

An example of Wi-Fi security in action is in public places, like cafes or airports, where many users use the same network. Such networks provide better security protection, using newer encryption algorithms (e.g., GCMP-256) and securing the handshake process more tightly to prevent attackers from listening to data interception downstream when upgrading it to WPA3. In addition, caution is recommended when accessing private information (like online banking) over public Wi-Fi, and suggestions for using virtual private networks (VPNs) go a long way toward limiting risk [6].

The solution comprises enhanced security encryption methods and best practice network security, making it perfect control for the National Security Department.

**Table 3: Summary of Wi-Fi Security Recommendations**

| • Security Practice | • Description |
|---|---|
| • Use WPA3 Protocol | • Ensures the use of the latest encryption standards |
| • Enable VPN on Public Wi-Fi | • Adds a layer of security by encrypting the data |
| • Disable Auto-Connect on Public Wi-Fi | • Prevents devices from automatically connecting to insecure networks |

## Challenges and Future Directions

Security practice evolution—Continuously adapting security practices as cybersecurity threats evolve, challenges change, and new organisational needs arise. This section considers the ongoing cyber security threat and offers future directions in light of new guidance on prevention, including individual and organisational interventions [7].

**• The Evolving Nature of Cyber Threats**

The security landscape is dynamic, and numerous new vectors of attacks or vulnerabilities are discovered daily. These attacks are becoming more sophisticated as threat actors adopt artificial intelligence (AI) and machine learning to create targeted, effective campaigns. For instance, the ransomware world has undergone marked developments concerning proprietary encryption techniques adopted by attackers, making data retrieval without payment difficult for targets [2].

As more products are interconnected and the number of IoT networks increases, cybercriminals have a larger and smarter attack surface than ever before. Cybersecurity—This challenge lies in the increasing market of smart home devices, which are not the most secure products. Because these devices are often not built with strong security, they make prime victims of an attack.

**• Balancing Security with User Convenience**

We need to balance robust security measures and user convenience in cyber security, which is a significant challenge. They suggest bolstering good security practices such as Multi-Factor Authentication (MFA) and regular updates but recognise that these can also impact the user experience. MFA, for instance, can lead to higher security by demanding extra verification steps, but fewer people want to use it since it is less convenient.

Most of the time, Wi-Fi security protocols such as WPA3 provide better security but might not support old hardware, which causes trouble when users have to use older devices. This means that when designing new cybersecurity counter-measures, we must also ask how these can be implemented in an extremely difficult way to break without compromising the usability of an interface.

**Table 4: User Convenience vs. Security Practices**

| • Security Measure | • Security Level | • User Convenience |
|---|---|---|
| • Passwords Only | • Low | • High |
| • Multi-Factor Authentication | • High | • Moderate |
| • Biometric Authentication | • High | • High |
| • VPN on Public Wi-Fi | • High | • Low |

**• Increasing Public Awareness and Education**

Non-technical issue: One of the biggest challenges facing cybersecurity daily is that the wider population needs more awareness. Users do not know the hazards of scams, unsafe wireless, and old installations. According to research on anti-phishing training systems, education is a significant help in making people more resistant to such cyber-attacks.

The next and most important step is to launch a cybersecurity information campaign. This campaign must address basic threats like phishing and ransomware and teach everyday internet user the importance of updating their software, using unique and strong passwords for each service/system they utilise, and providing informed guidance regarding safe browsing. Similarly, governments and organisations can provide free or discounted security tools—like antivirus software and VPNs—to incentivise greater adoption amongst the technically underserved.

**• Technological Improvements in Security Solutions**

In years to come, the latest trends in cyber security will emerge because of the rapid evolution in technology. Cybersecurity is where AI (Artificial Intelligence) and ML get widely applied, as automating threat detection and response can make a huge difference. So, artificial intelligence security systems can help examine vast amounts of information in real-time and recognise any uncommon tenant that was attacked. However, the bad guys commandeered those same technologies, increasing the stakes in an unending cyber turf war [4].

In addition, advancements in quantum computing could pose a great risk to classic encryption methods like RSA and ECC, which are common when people wish to secure their data or communications. Building quantum-resistant algorithms is an important research area for preserving the effectiveness of encryption in a post-quantum world.

## Conclusion

### The Significance of Cybersecurity

Cybersecurity is critical in our everyday lives as computers are used for most of our activities, including phishing threats, ransomware, unsecured WIFI networks, and vulnerable IoT devices. However, safeguarding personal data to protect privacy requires precautions and enforcement.

### Common Cybersecurity Threats

- New-school security awareness training helps you keep this pervasive threat at bay.
- The report also notes that ransomware attack vectors have continued to develop, and prevention would be most effective by following frequent backup policies and refraining from paying ransomware.
- It is well known that mobile devices and public Wi-Fi networks have been popular targets because they are so commonly used, and security procedures like safe browsing have to be continuously followed.
- Such new devices are known to open up new vulnerabilities, and in the case of smart homes, authentication should be strengthened along with updated firmware on these IoT devices.

### Technical Solutions

- Multi-factor authentication (MFA) and WPA3 are key to securing Wi-Fi networks and IoT devices.
- Phishing attacks can be nullified through anti-phishing education and training.
- Periodic upgrades, in conjunction with security practices and encryption on mobile and Wi-Fi networks, for better security.

### Challenges and Future Directions

- Finding the right balance between security and user convenience is always a tough task, as strict security might cause friction in the user experience.
- More general awareness of cybersecurity threats and special education are needed.
- This implies that there will be challenges and opportunities for cybersecurity in the future; however, he argued that technological advancements—such as AI, ML, or quantum computing—will never replace the human brain.

## References

1. Higashino M, Kawato T, Ohmori M, Kawamura T (2019) An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Information Leakage. 5th International Conference on Information Management (ICIM). https://doi.org/10.1109/infoman.2019.8714691.

2. Chesti A, Humayun M, Sama NU, Jhanjhi N (2020) Evolution, Mitigation, and Prevention of Ransomware. IEEE Xplore. Available: https://ieeexplore.ieee.org/abstract/document/9257708.
3. Nicholson J, Corner MD, Noble BD (2006) Mobile Device Security Using Transient Authentication. IEEE Transactions on Mobile Computing 5: 1489-1502.
4. Vegh L (2018) Cyber-physical systems security through multi-factor authentication and data analytics. IEEE Xplore. https://doi.org/10.1109/ICIT.2018.8352379.
5. Adnan H (2015) A comparative study of WLAN security protocols: WPA, WPA2. International Conference on Advances in Electrical Engineering (ICAEE). https://doi.org/10.1109/icaee.2015.7506822.
6. Roukounaki, Efremidis S, Soldatos J, Neises J, Walloschke T, et al. (2019) Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data: Towards End-to-End Security in IoT Systems. IEEE Xplore. https://doi.org/10.1109/GIOTS.2019.8766407.
7. Thomas M, Panchami V (2015) An encryption protocol for end-to-end secure transmission of SMS. International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]. https://doi.org/10.1109/iccpct.2015.7159471.