2022 Cybersecurity Best Practices to Prevent Cyber Attacks

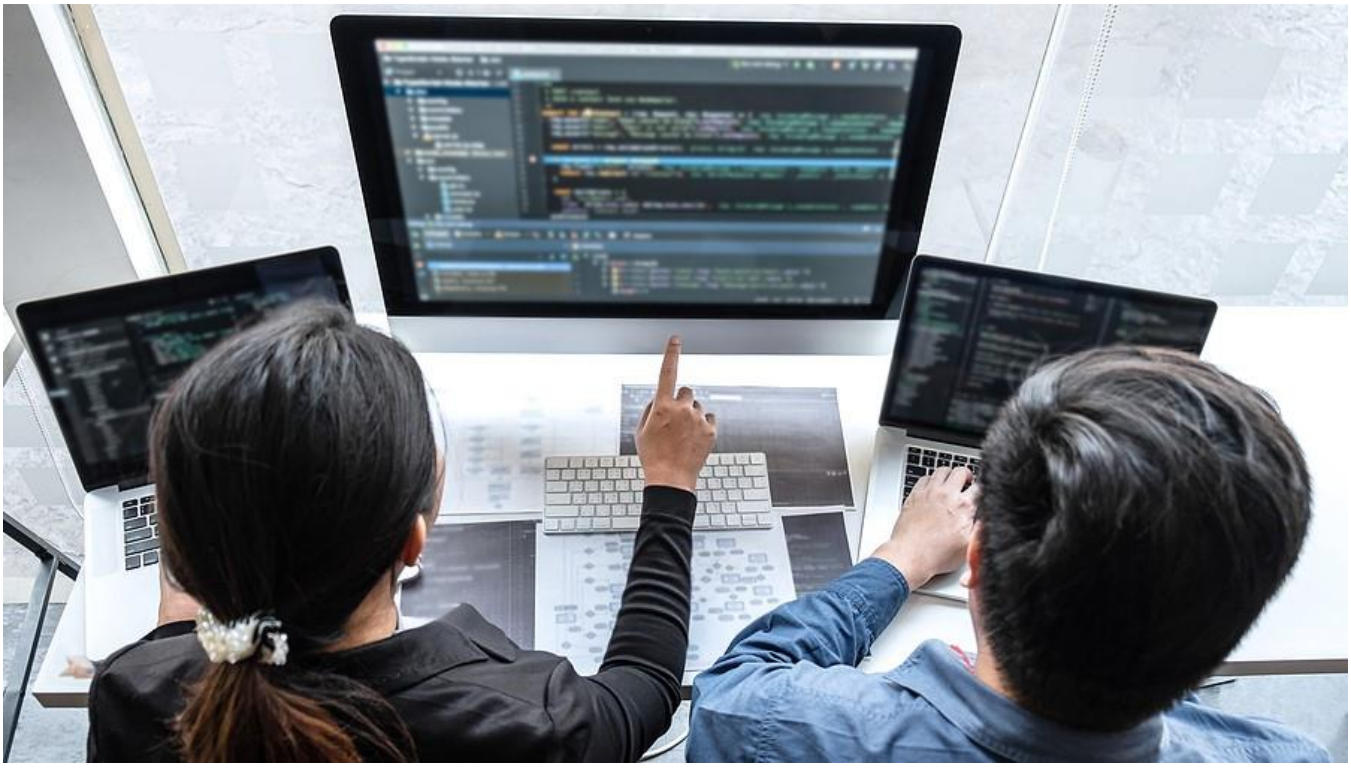
The experts have weighed in on predictions for cyber attacks in 2022. Most expect ransomware to increase in scope and sophistication. Supply chains, already under siege in 2021, will experience more focused attacks in the coming year. And both attackers and defenders will employ artificial intelligence as a key part of their 2022 cybersecurity best practices.

As organizations gear up to address these and other looming cyber threats, begin the new year right with a commitment to improved cybersecurity. With a multi-layered, comprehensive security strategy, organizations will protect vital assets and build customer confidence. Use these suggestions as a starting point to greater security.

1. Embrace Artificial Intelligence Tools

As cyber attacks grow more sophisticated, businesses must use increasingly sophisticated tools to fight them. Traditional methods for counteracting ransomware, including backups and email filters, remain critical. However, they do not provide adequate protection on their own.

Just as attackers leverage machine learning and deep learning tools, organizations must also build AI into their cybersecurity toolkit. Predictive intelligence solutions, for example, combine machine learning with big data analytics to automate threat protection.



2. Build Security Awareness

Once again, social engineering and phishing attacks account for a huge percentage of data breaches in 2021. And the shift to remote work appeared to increase both the occurrence of phishing attacks and the cost of data breaches. Consequently, effective security awareness training must play a role in cybersecurity strategy.

To make a difference, security education must involve a multi-faceted approach. This will include a mix of special events, ongoing formal training, and just-in-time reminders built into work processes. Training must be focused and specific, reaching users when and where they need it. For instance, phishing simulations and interactive training offer significant ROI.

3. Strengthen Endpoint Security

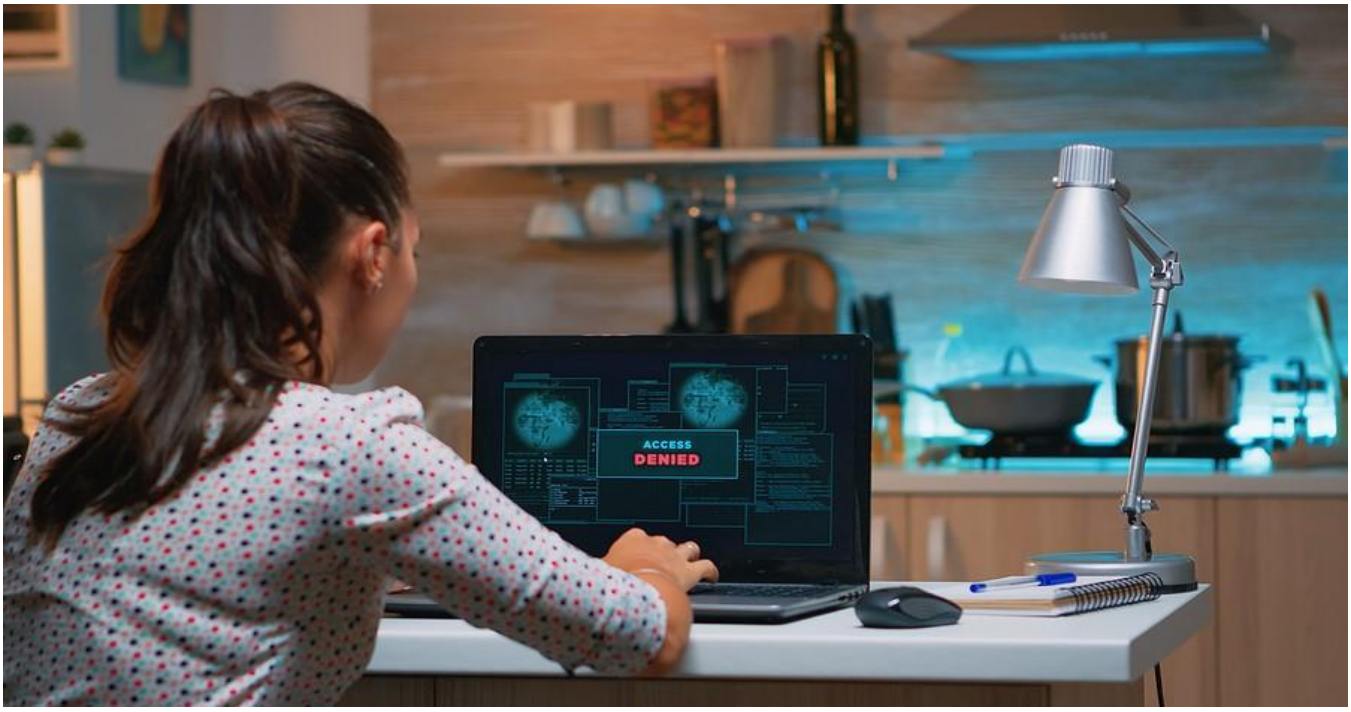
In addition to user education, a comprehensive cybersecurity strategy must address endpoint security. With remote and hybrid work apparently here to stay, the traditional security perimeter is a thing of the past.

For endpoint security, start with an audit of every device that can be given access to the network. Then identify and address potential vulnerabilities. This will include practices such as automating software updates to remote devices and implementing a zero-trust network.

4. Focus on Supply Chain

According to some experts, supply chain attacks will pose an even greater threat than malware in 2022. All of the attention on inhouse security will prove pointless if vulnerabilities introduced through a vendor leave an open door for attackers.

Carefully address cybersecurity with all third parties, building security policies into vendor contracts. Additionally, perform regular audits and continual monitoring of the supply chain.



5. Patch It Up

The recent Log4j vulnerability provided yet another reminder of the need to stay up to date on patches. Apply software and firmware patches quickly, automating those updates where possible. This applies to servers but also to all devices that access the system.

6. Implement Multi-factor Authentication

No list of cybersecurity best practices would be complete without a reminder of the importance of multi-factor authentication (MFA). Passwords no longer provide adequate protection. In fact, cyber insurance companies increasingly require organizations to implement MFA.

MFA usually involves three factors to verify identity: something you know, something you have and something you are. Examples of each include a PIN or the responses to a security question, a code from an authentication app and a fingerprint. This extra layer of authentication provides much stronger protection than traditional credentials.

Implement 2022 Cybersecurity Best Practices Without Delay

The cybersecurity experts at eMazzanti have the tools and expertise you need to design and implement a security solution tailored to your needs and budget. Whether you want to tap into the power of AI, improve user education, address endpoint security or implement MFA, we have the expertise to implement 2022 cybersecurity best practices.