

7 CYBERSECURITY RESOLUTIONS FOR 2022



LOADING ...

BAKE APP SEC TESTING INTO YOUR CI/CD PIPELINE

Getting applications and updates out quickly is important, but not as important is baking application security testing in the development phase before you launch your products.



PLAN A PENETRATION TEST

Detect flaws before an attacker does, run vulnerability management programs, identify/prioritize weaknesses, and run planned penetration test to find those weak spots in your cybersecurity.

DISCOVER HIDDEN REPOSITORIES

If you haven't hunted for data stores in non-standard locations, it's time you did. Find, classify, and secure data stores.



BE SURE TO LOCKDOWN FTP

Eliminate existing FTP instances and replace them with more secure alternatives. Adding layers of encryption protects sensitive or proprietary data in transit.

ADD MFA LOCKDOWN CREDENTIALS TO YOUR SYSTEMS

Adding multi-factor authentication (MFA) can significantly improve security. Credential thieves are locked out without the second factor.



DO PERIODIC TEST PHISHING

Conducting test phishing campaigns with meaningful feedback prepares your teams for this common attack by raising awareness throughout your organization.

OPTIMIZE & AUTOMATE

Simplify your operations through workflow automation to allow teams to quickly react to new IT challenges as they occur.



HOW TO COMPLETE YOUR LIST

Whether you were able to check off every item or your cybersecurity practices had a few empty boxes, the new year is a great chance is for fresh starts. By committing to your cybersecurity resolutions, you'll improve your program, and lead your organization move toward a better, more secure 2022.

Prepare for a secure 2022 with HelpSystem's expert panel discussion of 2021's cybersecurity challenges and offer advice on how to prepare for what is ahead.