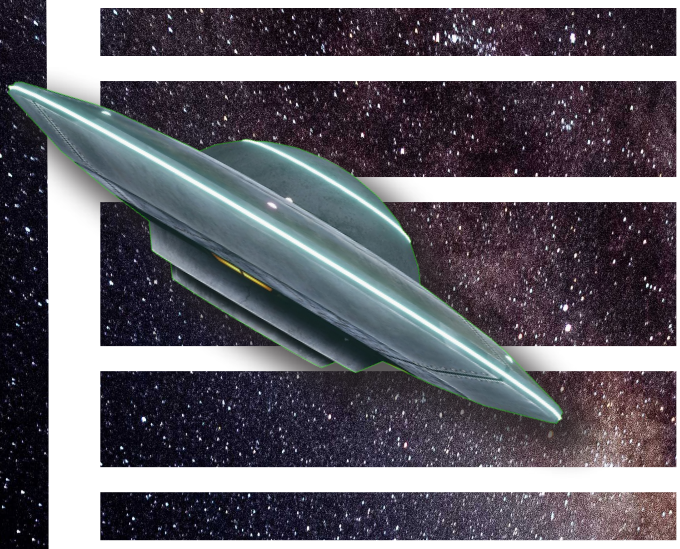
New Year's Resolutions

And Making "Space" To Keep Them

Office of Information Technology
Division of Information Security
JANUARY 2026



Making New Year's resolutions is a time-honored tradition. Unfortunately, breaking them is an even bigger tradition! Watch the expanded video here (January Newsletter Video) for tips to keep (and not break) those resolutions, but here's the gist:

Be Realistic

A realistic New Year's resolution is to pay attention to clues in phishing emails. You can look for tell-tale signs such as misspellings, emails being overly urgent, not wanting you to take a moment, and consider the legitimacy of the request. Such a resolution is realistic and one that you can keep.

Make a Plan

You can plan to verify requests for sensitive information before divulging it. Resolve to always verify email requests for sensitive information through secondary means, such as calling the requestor directly to confirm the request came from them. This New Year's resolution can spare you much grief.

Use Reminders

You can set reminders to ensure your software is up-to-date. A monthly calendar reminder can block out time so you can check that you have the latest version of all your programs to protect against cyberattacks.

Set Milestones

You can set milestones to back up files to your network drive at work as you progress on a project. Setting up milestones at the end of each stage, to back up important files from that stage, can ensure you don't lose any critical work.

Adjust as Needed

Remember that it's okay to adjust your resolutions as you go! Cybercriminals often change their methods, so you should adjust your plans to combat them. Stay up-to-date on what to look for by reading each monthly Cybersecurity Awareness Newsletter!

To report a cybersecurity incident, email Incident@ihs.gov. For any questions about this newsletter, contact Cybersecurity@ihs.gov.

And please watch the accompanying New Year's Resolution video for this newsletter, found here: January Newsletter Video!