New Year, New You, New Changes (Cybersecurity Resolutions 2022)

Office of Information Technology
Division of Information Security
JANUARY 2022

It's a New Year, which means it's another opportunity to set brand new resolutions that we can actually maintain. Every year cybercriminals persistently look for new ways to exploit security vulnerabilities and negatively impact our organization. It is our responsibility to take measures to deter or minimize the impact of cybersecurity attacks.

Here are seven resolutions you can easily incorporate into your daily work routine and make this year the safest one yet!

1. I will keep all my devices, browsers, and apps up to date.

By keeping your devices, browsers, and apps up to date, you can reduce exposure to new or existing security vulnerabilities.

Do not respond to email or internet requests to update or install a program on an IHS device. Please immediately forward these messages to Incident@ihs.gov.

IHS requests that all users proceed with installs or updates when they receive a computer-generated prompt on their IHS device.

2. I will think twice before opening suspicious attachments or emails.

If it looks suspicious, it could be a phishing scam. Someone may be attempting to steal personal information or hack your device. A phishing email may look familiar by claiming to be from a legitimate company or using the name of a person you may know. One of the best ways to detect a phishing attack is to verify the sender's identity. If you are unsure, do not reply or open any attachments. Be careful not to click on any links or parts of the email that may be disguised as links.

In addition to obvious links, there may be buttons or images containing links. Report it to Incident@ihs.gov immediately!

3. I will verify all requests for private information.

If you receive a request to provide private information, always verify the identity of the requestor and the purpose of the request. Cybercriminals are very clever in how they obtain information to compromise organizations.

4. I will back up critical files.

It is necessary to back up critical files in case primary storage becomes unavailable. To be prepared, store all critical files on a network drive or other IHS-approved storage option. Contact your local IT support for assistance. Check the storage drive or storage location periodically to ensure files are backed up.

5. I will properly protect sensitive information.

All IHS employees must follow policy and regulatory guidance regarding the amount of time information must be retained and when, and how, it should be deleted. Sensitive or critical data that is no longer required must be deleted using an acceptable utility program that overwrites the information in a secure manner. Contact your local IT staff for assistance. Properly place monitors to prevent public viewing. Use privacy screens where appropriate. Store hardcopy information in locked spaces when not in use. Immediately retrieve sensitive information from printers or faxes. Do not store sensitive information on SharePoint or a public shared drive. When storing sensitive information, make sure it is securely stored and only accessible to authorized persons.

Use the IHS Secure Data Transfer Service or encrypt the email with your PIV card to email sensitive information.

For additional information regarding the disposal of sensitive information at IHS please reference the IHS Disposition Schedule.

6. I will protect my password/PIN.

Do not share your passwords or PIN with anyone!

When creating your password, take your time, and don't repeat passwords across systems. Make sure your password is strong by using a combination of length, letters, numbers, and special characters (! @#$ %^&*), and avoid using personal information (birthdate, SSN, first name, last name, family members' names).

NIST encourages easy to memorize but strong passwords to discourage reusing passwords across multiple accounts or storing passwords insecurely, like in an unprotected file or on a sticky note. A good password should be easy to remember, but hard to guess.

Also, select "No" if a website or app prompts you to remember your password.

7. I will protect my data and devices.

Lastly, secure your items at all times, even if you'll only be away for a second. Whether you're at work or working remotely, secure your area before leaving your desk. Do not leave your items unattended when in public, and always take all portable items with you.

Don't use public networks. Hackers can use Bluetooth and public networks to access your information.

By sticking with these Cybersecurity resolutions all year long, you are helping to protect yourself and the entire organization from cyberattacks.

Please remember, if you see something suspicious, report it immediately to Incident@ihs.gov!

If you have any questions, please contact Cybersecurity@ihs.gov.