Personal Security Amid Cyber Chaos

Tips and Tricks to Stay Safe

Underwritten by Red Hat

govloop

Red Hat

Introduction

The SolarWinds attack rocked federal agencies. The Colonial Pipeline breach frenzied the country into a fuel rush. Then, President Biden issued an executive order, which maps out the future of cybersecurity for U.S. federal agencies and imposes new requirements for the private sector.

The new cybersecurity compass points the way of zero trust, cloud and identity-driven security. The Federal Risk and Authorization Management Program for clearing cloud contracts will also be reinvigorated.

The order's good news for government. But do you know where you fit into the picture?

Your agency will likely be training you soon, so you know exactly what the terms above mean and look like in practice. But likely, the biggest impact that you can make is doing the basics very, very well.

By the basics, we mean:

1. Not clicking on suspicious links
2. Choosing robust, diversified passwords

In the pages ahead, we'll help out. Starting with a quiz on passwords, we'll pitch a reliable, novel solution to password overload (trust me, we're feeling it, too). Then, we'll move onto what a phishing email is and how you can spot one.

Keep reading for this and more! You'll be happy you did – as will your agency.

Ransomware: A form of malware that deliberately prevents you from accessing files on your computer, holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered.

Passwords and Protections 101

"Open sesame! Abracadabra! Alohomora!"

Standard cybercriminal incantations shouldn't be enough to break your code. But when you set an easy password, with a standard phrase, no special characters and no backup checks, hackers can get in as easy as "1-2-3, open for me!"

Passwords are the front line of defense, the shield before the armor. In this section, we'll polish up your password strength and brush off misconceptions, adding a little glisten to your cyber suit.

First, let's put your password prowess to the test with a quiz from the feds.

Quiz

Answers are on the following page. Source: FTC

1. Which of these passwords is the most secure?

A. password
B. Password1!
C. P@$$w0rd1!
D. Grouchyc@tl@serPointer!

2. True or false: You should use the same password as much as possible so you don't forget your login.

3. Where is a good place to store your passwords?

A. On a piece of paper
B. In a password manager
C. In a notes app
D. All of the above

4. Which of the following does a password manager NOT do?

A. Randomly generate tough-to-crack passwords
B. Store passwords in a central database so that you can access them when you need
C. Scroll through your existing passwords and tell you the ones that need work
D. Ask for a master password to access your information

5. Which one of these statements is true?

A. It's best to use multifactor authentication to access areas of the network with sensitive information.
B. You should use the same password for key devices to guarantee that high-level employees can access them in an emergency.
C. The best way to protect data is to make sure no one loses any device.
D. You shouldn't limit login attempts on key devices, because getting locked out for having too many incorrect attempts would leave you unable to access your accounts.

Answer Key

1. **D.** The National Institute of Standards and Technology (NIST) recommends you create passphrases that are "easy to associate in your mind, are personal to you and preferably visual in some way," such as "grouchy cat laser pointer." These are easy for humans to remember and difficult for computers to guess. Always back them up with another layer of protection, like multifactor authentication, when possible.
2. **False.** If someone gets one of your codes, you don't want them to get everything else. That's not to say you can't have favorites, but especially for important information, consider using unique combinations or a password manager.
3. **B.** You don't want cybercriminals or brick-and-mortar criminals to pinch your information. So a notes app and notepad are both too susceptible to easy access. Use a password manager instead.
4. **C.** A password manager does a lot, but it's up to you to determine the services you use and which existing passwords you have. It does, however, randomly generate complicated passwords and save them for the right website. All of that information is stored centrally, accessed with a master password.
5. **A.** Always use multifactor authentication to access areas of your network and devices with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone, or a key that's inserted into a computer.

The Elements of a Strong and Sturdy Password

North Dakota: "Passwords are keys; guard them like you guard your house key."

Maricopa County: "Think of your password like your toothbrush: Change it regularly and don't share it."

So what makes a good password?

Maricopa County

- Passwords should be easy to remember, but hard to guess.
- Passwords should not be written down.
- Passwords should be at least eight characters long, containing mixed-case characters and special symbols or numbers.
- Passwords should not be easy-to-guess key sequences (e.g. "qwerty").
- Passwords should not be dictionary words.

North Dakota

Our network and software security and firewalls can be the best and yet, if someone obtains our password, all the security in the world will not protect our data.

Do not include:

- Names
- Birthdates
- Seasons
- Hometowns
- Favorite team names, etc.

Hackers focus on the region of their potential victim, so they may try Fall2019, Vikings1, Packers1, Fargo2020, etc. as password attempts.

How to Manage All of That

Here's where we run into trouble. We can follow these rules of thumb, and still stray from safety because we need so many passwords, with different requirements or different codes. So what do you do?

Password Manager: "Programs called password managers offer the option to create randomly generated passwords for all of your accounts. You then access those strong passwords with a master password." – Cybersecurity and Infrastructure Security Agency

What should you look for when seeking a password manager solution?

- **Lock-In Period:** Can you easily switch your information to another product if you don't like the first one?
- **MFA:** Does it support multifactor authentication?
- **Cross-Platform Capabilities:** Does it support each device platform you use?
- **Mobile Device Features:** What mobile device features does it have? For example, does it have biometric options instead of complicated passcodes?
- **Management:** Does it have a browser toolbar or menu to manage multiple saved accounts?
- **Autofill:** Will it autofill forms similar to your web browser?
- **Usability:** Is it easy to use?

What to watch out for

- Forgetting the master password – your account login info can be lost for good
- Password managers that don't automatically capture updated password events
- Logging in with your secure username and password to a website that doesn't use a secure HTTPS connection
- Default generated passwords that are not at least 20 characters long and include all of the major character types – uppercase, lowercase, numbers and symbols

Bonus Features: With advanced/ premium options, it could:

- Manage passwords for applications
- Automate the password change process
- Securely share passwords with other users, preferably with advanced permissions, for when users are on a single or controlled account
- Offer large-scale secure storage
- Have built-in virtual private network

Source: Maricopa County

How long would it take for a high-powered server to guess these passwords?

- Today123 – 36.99 minutes
- Today1234! – 19.24 years
- Mi55ouriR!v3r – **1.65 hundred thousand centuries**

Source: North Dakota

Catch a Phish(ing Attempt)!

Besides passwords, the other major cybersecurity threat you'll encounter on a regular basis is phishing attempts – you know, those spam emails and texts that swim into your inbox. Well, attackers are getting smarter, so with that in mind, try catching the folly in this phishing attempt below.

Sometimes, you can tell from the address alone what's going on. The jig is up right here. Why would the official company have an odd address with numbers like this one? Still, keep reading.

From: cloudservicesteam45@gmail.com

Subject: Your Account Info

Hi Friend,

We've noticed some unrecognized activity going on on your Web Client account.

As a result, we've locked your account.

To open it up, you'll need to provide us with your account information and proof of identification. It's an easy process; just respond to this email.

– Your Cloud Services Provider

Be wary of emails that target account information. To check if they're real, don't be afraid to independently look up the company phone number and ask if this email is from them.

Notice the generic opening. That's unusual for a company with your information. This could be so that they can send the same email to lots of addresses.

Odd capitalizations and phrasings can be a dead giveaway. At big companies with large marketing departments, mistakes wouldn't get by.

Is your account actually locked? Don't be afraid to close the email and go to the page you have gone to before to log in.

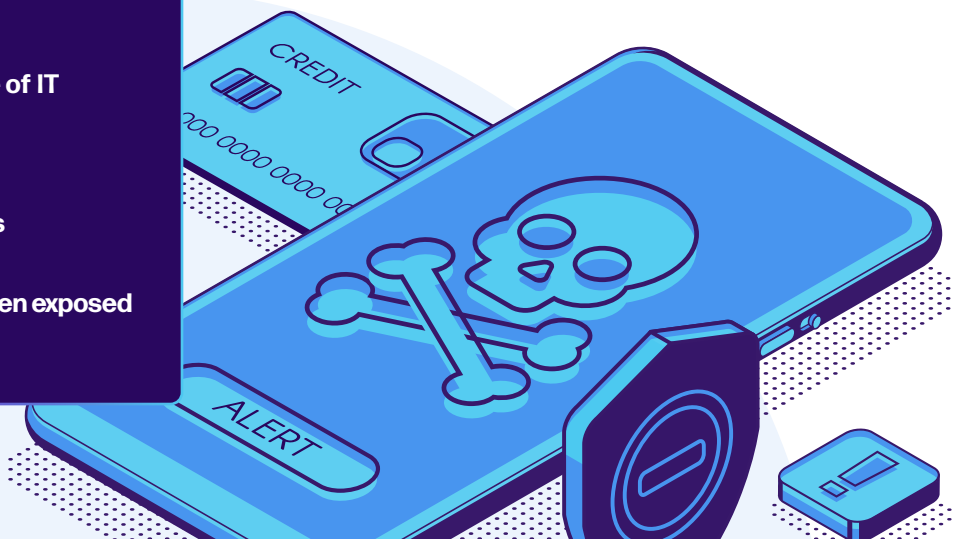
This information is almost never solicited by email from reputable sources. Safe to say, you should forward this to your security team and delete it from your inbox.

NEVER:

- X **Respond with information**
- X **Click on links**
- X **Download attachments**
- X **Share with colleagues outside of IT**

ALWAYS:

- √ **Avoid any links or attachments**
- √ **Report to proper channel**
- √ **Inform others who may have been exposed**
- √ **Delete the email**



INDUSTRY SPOTLIGHT

Dealing With Complexity in a Tangled World

An interview with Michael Epley, Chief Architect and Security Strategist, North America Public Sector, Red Hat

Technological advances have driven the workforce and humanity to new heights, even enabling a society that functions largely digitally during a pandemic. But the proliferation of applications, accounts and the like creates new challenges for security – a more-tech-means-more-problems conundrum.

Unmistakably, technology has become more complex. Instead of one smart device, you likely have several. Instead of one password, you probably have an array. Instead of one login screen, you often have to go through multiple gates.

Security is scrambling to keep pace in the innovation race, and try as it may, it often strays behind. There's just so much to secure, and with the infamous cyber skills shortage in government, teams don't have enough hands for it all.

"There's a tremendous amount of complexity involved here," Michael Epley, Chief Architect and Security Strategist for Red Hat's North America Public Sector. "It's very difficult to get people that can look at all those different systems and integrate, or tie them all together, safely."

But security isn't locked into a losing battle; it can still catch up.

Relearn the practice

Imagine someone strolling through an apartment lobby and pressing on door handles until they find an unlocked room to ransack. That's what hackers try inside networks.

To make it more difficult, agencies need constant security checks – at the front door, in the elevator and for each individual room.

Zero standing privileges is a concept that prevents guaranteed entry. It's an extension of the least-privilege model and paves the way for a zero-trust security strategy, which constantly asks users to verify identity.

Layered on top, privilege access management ensures on-demand access for users after they prove they need it. Criminals are locked out, and users can access the room they need.

Verify identity

Having more locks makes no difference if one key opens them all. In other words, users need more than one way to verify their identity.

Identity checks now rely on multifactor authentication, an example being a texted code. The problem here is that employees don't want to be treated as strangers in their own agencies.

An easy way for agencies to maintain security without encumbering employees is biometric authentication, like fingerprint and facial ID, Epley said. These secure and easy-to-use MFAs don't impede productivity and promote acceptance, not circumvention.

Don't go alone

Agencies need data from all their services working together to beat back attacks, but integration is no small feat. For that reason, many are looking for ways to manage the complexity of securing their enterprises.

Turning to managed security services is one strategy facilitated by cloud platforms. Managed services essentially outsource security – as completely or partially as agencies would like in areas like zero trust – while still giving agencies control of their data and policies. Combined with clearinghouses for intra-agency risk and threat analysis, these services respond quickly to their environments.

"You're using a managed service that's presumably provided by an expert in that particular piece of technology. That's why you're starting to see a rise of more managed services," Epley said.

Red Hat

We know the landscape, and how to innovate in it

Modern security means shifting from a strategy of minimizing change to one that is optimized for change.

www.redhat.com/gov

Next Steps

Cybersecurity isn't a one-trick pony. The tips and tricks outlined in these few pages are only small parts of how to safeguard your personal and professional lives.

The other factors can be found in "Your Cybersecurity Handbook: Tips and Tricks to Stay Safe." There, you'll explore the other parts, and we walk you through with fun activities, games and even a crossword puzzle.

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop