October: Cybersecurity Awareness Month

Since 2004, October is celebrated as Cybersecurity Awareness Month, previously called National Cybersecurity Awareness Month. The President of the United States and Congress have declared October to be Cybersecurity Awareness Month, helping individuals protect themselves online as threats to technology and confidential data become more commonplace.

Now in its 19th year, Cybersecurity Awareness Month is a collaborative effort between government and industry to raise cybersecurity awareness nationwide and help ensure that all have the resources they need to be safe and secure online.

October is Cybersecurity Awareness Month, which gives security leaders and executives an opportunity to raise fresh ideas and conversations around cybersecurity.

Cybersecurity Awareness Month Theme:

"See Yourself in Cyber "

This year's campaign theme — *"See Yourself in Cyber"* — demonstrates that while cybersecurity may seem like a complex subject, ultimately, it's really all about people.

This October will focus on the “people” part of cybersecurity, providing information and resources to help educate partners and the public, and ensure all individuals and organizations make smart decisions whether on the job, at home or at school – now and in the future. To engage in this year’s efforts by creating own cyber awareness campaigns and sharing this messaging with peers.

- For individuals and families, we encourage you to **See Yourself taking action to stay safe online.** That means enabling basic cyber hygiene practices: update your software, think before you click, have good strong passwords or a password keeper, and enable multi-factor authentication (meaning you need "More Than A Password!") on all your sensitive accounts.
- For those considering joining the cyber community, we encourage you to **See Yourself joining the cyber workforce.** We'll be talking with leaders from across the country about how we can build a cybersecurity workforce that is bigger, more diverse and dedicated to solving the problems that will help keep the American people safe.
- For our partners in industry, we encourage you to **See Yourself as part of the solution.** That means putting operational collaboration into practice, working together to share information in real-time, and reducing risk and build resilience from the start to protect America's critical infrastructure and the systems that Americans rely on every day.

4 Things You Can Do

Throughout October, highlight key action steps that everyone should take:

- **Think Before You Click: Recognize and Report Phishing:** If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
- **Update Your Software:** Don't delay -- If you see a software update notification, act promptly. Better yet, turn on automatic updates.
- **Use Strong Passwords:** Use passwords that are long, unique, and randomly generated. Use password managers to generate and remember different, complex passwords for each of your accounts. A passwords manager will encrypt passwords securing them for you!
- **Enable Multi-Factor Authentication:** You need more than a password to protect your online accounts, and **enabling MFA makes you significantly less likely to get hacked.**

Recognize and Report Phishing

- Have you ever seen a link that looks a little off? It looks like something you've seen before, but it says you need to change or enter a password. Or maybe it asks you to verify personal information.

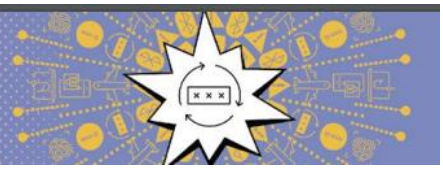
▪ It's likely a phishing scheme: a link or webpage that looks legitimate, but it's a trick designed by bad actors to have you reveal your passwords, social security number, credit card numbers, or other sensitive information. Once they have that information, they can use it on legitimate sites.

Update Your Software

- Bad actors will exploit flaws in the system. Network defenders are working hard to fix them as soon as they can, but their work relies on all of us updating our software with their latest fixes.

▪ Update the operating system on your mobile phones, tablets, and laptops. And update your applications – especially the web browsers – on all your devices too. Turn on automatic updates for all devices, applications, and operating systems.

Use Strong Passwords



- Creating strong passwords is an easy way to improve your cyber security. Strong passwords include one uppercase letter, one lowercase letter, at least one number and 11 or more characters. Be sure to use different passwords for different accounts.

▪ Use password managers to generate and remember different, complex passwords for each of your accounts. A password manager will encrypt passwords securing them for you!

▪ Put cybersecurity first by protecting the information stored on devices. Much of a user's personal information is stored either on their computer, smartphone, tablet or possibly someone else's system.

- It's More than a Password: Why We all Need Multi-factor Authentication

▪ If you can do just one thing to protect your online valuables, set up Multi-factor Authentication.

▪ It goes by many names: Two Factor Authentication. Multifactor Authentication. Two Step Factor Authentication. MFA. 2FA. They all mean the same thing: opting-into an extra step when trusted websites and applications ask you to confirm you're really who you say you are.

Report incidents, phishing attempts, malware, and vulnerabilities.

Cybersecurity is everyone's job — but, sometimes, it can be difficult to get people engaged around security and best practices. But with the escalating volume and frequency of global phishing and social engineering attacks, each employee's decisions are more impactful than ever.

Here are 31 cybersecurity tips — one for each day of Cybersecurity Awareness Month — to spark some creative thinking around how you can foster greater security awareness at your organization.

1. Ditch your reused passwords.

Data breaches often leak user credentials, including passwords. This can be hugely damaging for people who reuse the same passwords across accounts — and each additional account amplifies your risk. Protect yourself by using a password manager to create complex, unique passwords for each account. This might be a weekend project for some, but it's absolutely worth the effort, and a great way to start off Cybersecurity Awareness Month. For more security tips, check out our Empowered Employee Report.

2. Check your security settings.

A staggering amount of information is sent via email every second, so it's essential that all that data is properly secured. For practical ways to get started, check out our guide for 5 steps to secure your data in Gmail.

3. Apply multi-factor authentication.

It may add an extra step to your login process, but it's well worth the extra 2 seconds. This way, if someone gets a hold of your password, they won't be able to access your accounts without access to your phone or other verification information. Check out other best practices for email security.

4. Understand end-to-end encryption and how to use it.

End-to-end encryption ensures your data remains safe from the moment it's created, to the moment it's shared. Check out our blog for the answer to the question, "What is end-to-end encryption?"

5. Add end-to-end encryption to your email.

Email encryption doesn't have to be cumbersome. In fact, it can be an easy, natural part of users' workflows. Try Virtru email encryption free for 2 weeks to see how simple data protection can be.

6. Slow down.

We're all busy. But slowing down before you open an email, or thinking twice before you click on a link, could be the difference between a close call and a massive data breach. We sat down with KnowBe4's Roger Grimes, who shared some great insights for spotting and preventing phishing and social engineering attacks — and his interview is a great resource to share with employees for Cybersecurity Awareness Month. Check out our interview on the psychology of social engineering.

7. Make cybersecurity accessible.

As we mentioned above, cybersecurity is everyone's job. Are your teams equipped with simple tools and a clear understanding of their role in protecting data? Our Empowered Employee Report contains tips for selecting easy-to-use data protection tools, as well as our recommendations for getting teams invested in security — conversation starters, communication advice, and more.

8. Secure your cloud-hosted data.

Did you know that you can shield your cloud-hosted data from third parties — including the cloud providers themselves? Virtru data protection makes this possible: As an example, we are a Google-recommended key management partner for Google Workspace Client-Side Encryption. Check out our blog post on 5 myths surrounding cloud migration, and how you can ensure total privacy and control of your data in the cloud.

9. Unusual requests are red flags.

Even if an email appears to come from someone you know and trust, be cautious of any message that asks you to do something that could put you or your organization at risk — even if it appears to come from your boss or an executive. Phishing attacks now commonly use industry-specific terms, jargon, and client scenarios to foster a false sense of trust. As they learn, hacking groups can make these emails look increasingly realistic. Learn more in our blog post on social engineering.

10. Focus on the most impactful priorities.

“Everyone is seeing threats like bubbles in a glass of champagne, and they’re not being told, ‘Two of those bubbles matter more than all the other bubbles.’ Because of that, they’re not focusing correctly,” says KnowBe4’s Roger Grimes, author of A Data-Driven Computer Defense. Those two most important “bubbles” have been the same for 30 years, he says: social engineering and unpatched software. Discover more insights on how to effectively prioritize your security efforts in our Empowered Employee report.

11. Assess data protection across departments.

Whether you’re a global manufacturer, a small retail shop, a healthcare provider, a school, or a non-profit organization, you have sensitive information that hackers can profit from, and that data can be found across every corner of your business. Every department needs data protection. Have conversations with team members across every department to get a sense of the kinds of sensitive information they’re handling, and whether it’s being protected: Employee and customer information, proprietary strategic data, financial records, PHI, PII, and more. You might be surprised by how much data you uncover.

12. Construct a safety net for human error.

We’re all human. We’ve all made mistakes around cybersecurity. The question is — when mistakes happen, what tools do you have to mitigate or prevent damage? Virtru helps you implement two valuable safety nets for human error: Data Loss Prevention rules that automatically encrypt certain types of data by default, and a “Revoke” feature, which lets you revoke access to shared data at any time — even if that data has already been shared and accessed outside your network. This helps you take immediate action to mitigate your risk.

13. Revisit your breach prevention plan.

With ransomware attacks and data breaches on the rise, it’s important to ensure your breach prevention and response plan is up to date, and that everyone understands their role in preventing and responding to an incident. When evaluating your breach

prevention plan, ask yourself: Are we just protecting our systems and networks, or are we protecting the data itself, everywhere it travels?

14. Examine how you manage and share customer data.

Most companies have some kind of Customer Relationship Management (CRM) software to maintain client data. This information is often sensitive in nature, containing personally identifiable information (PII) and credit card/billing information. Ensure the data flowing through those platforms remains secure. For more on how to protect customer data, listen to our recent webinar on adding a layer of encryption to your SaaS applications.

15. Build trust with a commitment to security.

Trust can be your competitive advantage. In a world where so many companies take a lax approach to protecting their users' privacy, you can build stronger relationships by demonstrating a commitment to security — for your customers, employees, and partners. Cybersecurity Awareness Month presents a great opportunity to communicate this with your audience, as well. Discover six ways to protect customer data and win trust.

16. Bridge the gap between work and home.

By highlighting the risks of ransomware to employees' personal as well as professional lives, security teams can convey the consequences of cyber attacks in a more tangible way. When individuals understand the potential personal impacts of a data breach — such as the compromise of their own personal accounts — they'll start to take security more seriously. Our Empowered Employee Report includes conversation starters and tips for connecting with employees.

17. A Zero Trust strategy creates maximum confidence.

Zero Trust treats every user and every system with equal caution. Everyone is on the same playing field, and it frees up your organization to create and collaborate with greater confidence that their data remains safe. Check out our tips for explaining Zero Trust to employees during Cybersecurity Awareness Month.

18. Know who holds the keys to your data.

For strong security, you'll want to manage your own encryption keys — or select a trusted partner who can manage them for you, separately from your data. Check out our encryption key management guide for details on how to evaluate the right key management framework for your organization.

19. Highlight your organization's security heroes.

Have an IT team of rock stars? What about colleagues who do a great job of encouraging strong security behaviour among their peers? Celebrate these employees and give them some well-deserved recognition. This can go a long way to cultivate openness and engagement around cybersecurity. Download our Empowered Employee Report for more tips for fostering an engaged culture.

20. Calculate how much data is leaving your organization.

Data flows in and out of organizations at high velocity. It's important to understand just how much data is being shared externally so you can effectively protect it. Use the Virtru Data Sharing Calculator to understand your potential risk for a breach — and learn how you can mitigate the impact.

21. Find your cybersecurity advocates.

You know those colleagues who are always the early adopters of new technology? How about those who are passionate about block chain, or ethical AI? These can be your most powerful cybersecurity advocates. Harness the passion and interest of these individuals to help your organization adopt a consistent, strong security mind set — one of continuous learning and knowledge sharing. After all, data security is everyone's responsibility.

22. Start an insider threat prevention program.

Most companies face far more danger from lack of attention or training by insiders than from actual malice, but it's still crucial to understand the security risks both pose. Fostering a collaborative culture of security will earn employee buy-in, and provide better results (and morale) than a top down "everyone's a suspect" approach. Check out our Guide to Creating an Insider Threat Program for tips on how to cultivate engagement.

23. Make it easy to collaborate securely.

For your teams to actually use your security tools, they have to be easy to use. In a Virtru case study, Chartered Management Institute's Information Security Manager, Leroy Cunningham, said it well: "It's great having all the bells and whistles, but if your end users don't know how to use it, they won't use it, and it's as simple as that. I like how clean and simple Virtru's product is, it's a simple toggle switch to turn it on or off, and it gives us more autonomy." Read our Chartered Management Institute (CMI) case study to see how they used Virtru to help break down data silos.

24. Approach security conversations with positivity.

There's enough messaging around fear, uncertainty, and doubt in the cybersecurity world. We've found it's far more effective to empower teams with simple tools, clear

education, and positive messaging that gives them the confidence to do their jobs while protecting data. Page 3 of our Empowered Employee report contains several tips to evaluate the way you position your security messages to teams.

25. Examine your supply chain connections.

Whether it's third-party software or hardware throughout the enterprise supply chain ecosystem, even "trusted" networks quickly become a risk in the absence of data access controls. Here are some of the supply chain risks to be aware of, and why data-centric access controls can help you mitigate those risks.

26. Connect with the "why."

For schools, it's protecting students' safety and privacy. For healthcare providers, it's safeguarding patients' well-being. For companies, it's protecting confidentiality and maintaining trust. Whatever your "Why" is, it's vital to make that a central part of your story for the importance of protecting data.

Our "Why" — helping create a world where your data remains under your control, everywhere, without limiting your ability to innovate, share, and collaborate.

27. Don't overlook data flowing through SaaS apps.

The average enterprise has over 500 applications, and every app amplifies your risk. Determine which of those applications transmit sensitive data (e.g., customer records, employee PII, data for analytics), and evaluate whether that data is being protected everywhere it's shared. See how Virtru can help you apply a layer of encryption for apps like Salesforce, Zendesk, and Looker.

28. Make it simple for distributed teams to share information.

More teams than ever are moving to a remote-first or hybrid environment. These distributed teams need sophisticated tools to collaborate and share information quickly — with both internal and external partners. Secure Share encrypted file-sharing platform makes it simple for teams to send and receive information with external partners (like clients, business partners, board members, and others) with the confidence that it's always protected.

29. Secure data management makes a strong first impression.

The competition for top talent is high — and it's important for companies to make a strong first impression on prospective new hires, both during the interview process and during on boarding. Show that you take security seriously and are committed to

protecting their private data. Read our blog for more information on how HR teams and hiring managers can protect on-boarding data.

30. Make sure you're protecting employees' COVID-19 vaccine and test results.

Many HR teams are still collecting and managing COVID-19 vaccine and test data. That information can remain on file, but it may also need to be communicated to managers and team leaders. If that information needs to be shared via email or other collaboration flows, it's essential that those messages are secured with end-to-end data protection. Our blog post provides some recommendations for securing employees' private COVID-19 vaccination and test data.

31. Continue the cybersecurity conversation year-round, not just during Cybersecurity Awareness Month.

The key to engaging your employees around cybersecurity is to make security a habit, an everyday part of your organization's life. Just like any other habit, it's about small, continuous shifts that add up to a big impact.