

The background is a solid dark blue color. It is decorated with several white snowflake icons of varying sizes and orientations. Additionally, there are numerous semi-transparent light blue circles of different diameters scattered across the entire background, creating a bokeh or 'snowfall' effect.


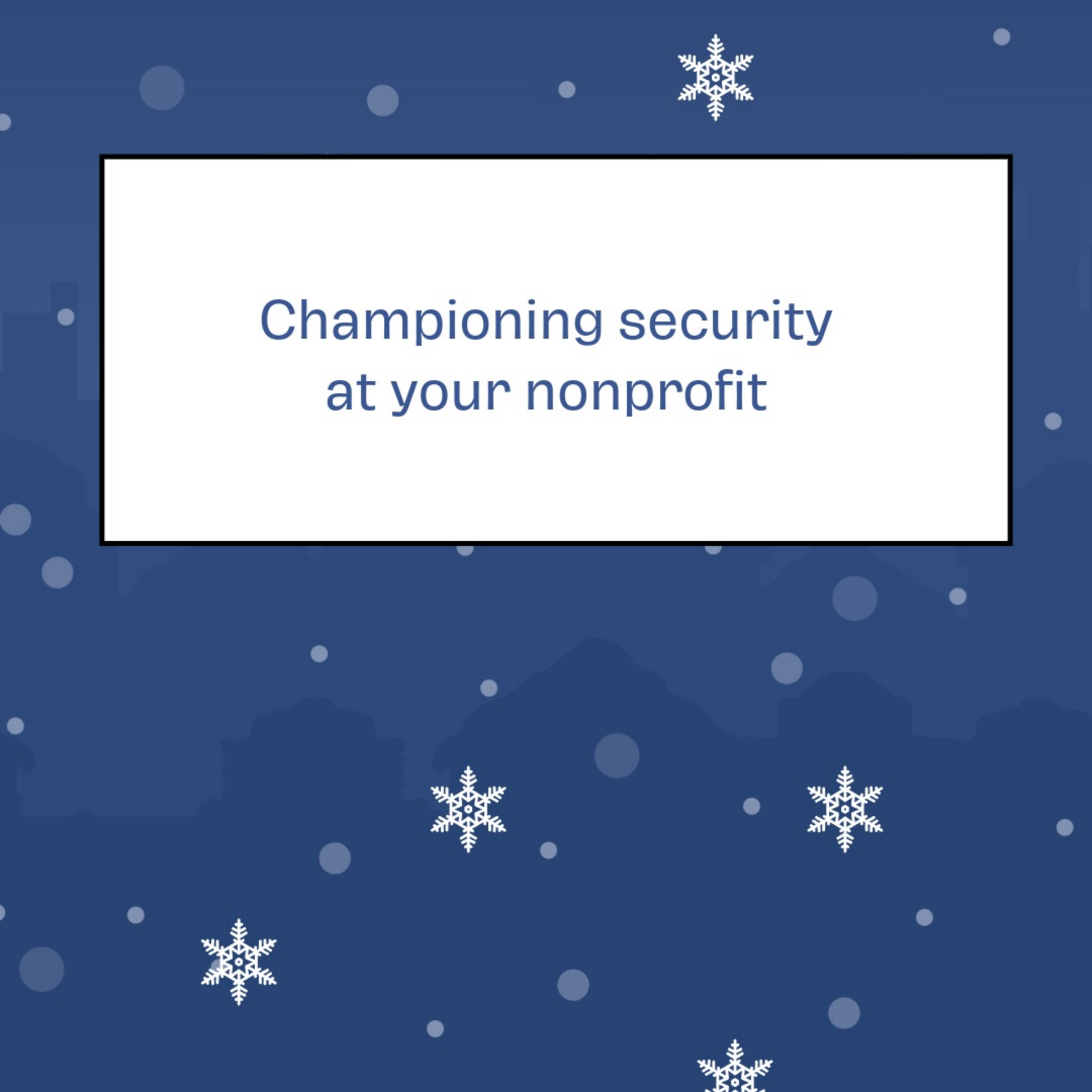
# How to talk to your team about cybersecurity



**501 Secure.org**

Cybersecurity Assistance for Nonprofits





# Championing security at your nonprofit



If you're stepping up to champion security in your organization, you might worry that you don't know enough to talk about "cybersecurity". But you don't need to be an expert to initiate a conversation that leads to increased awareness and safer work practices among your colleagues.

Online security is no longer just IT's job; it's the responsibility of anyone who uses the internet for work.







If you're worried about your lack of technical chops, remember that your team doesn't have to take only your word for it. Support your talk by sharing online safety information from reputable sources. Incorporate the latest expert insights from free annual cybersecurity reports published by well-known and trusted vendors.

You'll find a list of shareable resources in our free Holiday Preparedness Toolkit at <https://www.501Secure.org/Toolkits>.





It can be difficult to get colleagues to focus on security just before a holiday vacation. So keep it simple and non-technical with a friendly checklist.

Provide them with a set of easy-to-complete tasks that lock the digital doors before your team takes their leave. Every team member, device, and account you help secure is progress toward reducing risk and increasing awareness and good habits.





# Nonprofit vulnerabilities during the holidays







The holidays are a busy and distracting time for nonprofits. Team members head out on vacation leaving lots to do with less staff to do it.

Whether it's the skeleton crew keeping the lights on or team members checking their work email via their phones while on vacation, cybercriminals know your team's guard is down.





Social engineering attacks can be easily misjudged amidst the flurry of delivery notifications, purchase confirmations, out of office emails, and last minute tasks.

**Your organization is not too small to be targeted.** Criminals use automated tools to scan the internet for easy access points; they seek any opportunity to exploit.







Unsecured personal devices used for work may leave the door open to phishing attacks that compromise business accounts.

Account break-ins during holidays and weekends may go unnoticed until team members return and find themselves locked out.





Even if your organization has not yet implemented a security program or does not yet have professional IT support, there are a few simple steps that can reduce the risk of data loss or a cybersecurity incident during the holiday vacation season.

You'll find a checklist in the Holiday Preparedness Toolkit that you can share with your team.





Follow these steps to prepare to talk to your team:

1. Gather information and helpers
2. Schedule a brief meeting with your team
3. Share the checklist and a deadline to complete it (to build in accountability)
4. Follow up with an email reminder
5. Get confirmation from each team member that they've completed the checklist







## 1. Meeting preparation

a) Involve leadership when possible.

A quick email or endorsement from a senior manager reinforces the importance of security and transforms it from a personal chore into an organization priority.

Whether or not you get a formal sign-off, talking to your team begins a conversation that raises awareness and encourages participation.





b) Coordinate directly with your IT team.

If you have an IT team or staff member who provides IT services, ask them to review the full checklist to ensure technical accuracy and consistency with any existing policies.

IT support may receive an increase in requests for assistance with tasks like setting up MFA or clearing the browser cache.

Coordinating with them ensures they are prepared for a temporary surge in support requests.





c) Review the shareable resource list for cybercrime facts relevant to your team.

You'll find free, easy-to-read publications with the latest statistics on cybercrime activity, examples of methods cybercriminals are currently using, and recommended actions.

These are non-technical sources by reputable software vendors published annually. If possible select a report from a vendor familiar to your team, such as Microsoft's Digital Defense Report or Google's Cybersecurity Forecast.







Focus on sharing the latest information about social engineering, phishing, account and device security.

And talk about how these methods may impact the specific work processes, software, and data your team uses everyday. Let team members share about incidents they've experienced or phishing attempts they've noticed.

Encourage open, nonjudgmental conversation. Establishing emotional and social safety to report security troubles is just as important as implementing long passwords and MFA.





## 2. Schedule a brief meeting with your team

### Suggested Email:

We're holding a mandatory "Worry-Free Vacation Security Huddle" this week.

To ensure everyone can fully disconnect and enjoy their time off, we will review a simple checklist for securing your devices and accounts before you leave.

Looking forward to seeing you all there so we can close out the year securely!





### 3. Share the checklist during the meeting and walk through each step

a) Distribute the checklist as a PDF.

Or load the checklist into a form tool (such as Google or MS Forms) and distribute via link. Your team can submit the form as confirmation.

Add a checkbox to the form to indicate an item is complete.







b) Walk through each item in the checklist and give your team time to ask questions.

c) Demonstrate how to complete each task. For example, show your team exactly where to enable MFA in the online software you use. Or provide an example of an acceptable long password.

You may want to invite a member of your IT team to participate in the meeting to help with questions and demonstrations.

You'll find an editable checklist in the Holiday Preparedness Toolkit.





## 4. Follow up with an email reminder

### Suggested Email:

A quick reminder before you leave on holiday. If you have not done so already, please take 5 minutes to complete the Holiday Preparedness Checklist that we reviewed this week. Let me know when you've completed it.

Thank you for your help in securing our organization while everyone is out.

Enjoy every minute of your vacation—you've earned it!





5. Get confirmation from each team member that they've completed the checklist.

Follow up personally with those who haven't confirmed to offer assistance or answer questions they may have about the list or security.







501Secure's 2025 holiday preparedness toolkit includes:

- How to talk to your team about cybersecurity
- Holiday preparedness checklist
- Shareable expert information resources
- Email templates
- Meeting agenda

Download your free copy of at  
[www.501Secure.org/holiday-readiness-toolkit](http://www.501Secure.org/holiday-readiness-toolkit)

