12 Tips to Stay Safer Online

October 16, 2018

techsoup

Using ReadyTalk

- Chat to ask questions
- All lines are muted
- If you lose your Internet connection, reconnect using the link emailed to you.
- You can find upcoming and past webinars on the TechSoup website: www.techsoup.org/community/events-webinars
- You will receive an email with this presentation, recording, and links
- Tweet us @TechSoup and use hashtag #tswebinars

A Global Network Bridging Tech Solutions and Services for Good

Where are you on the map?

● Countries Served ● TechSoup Partner Location ● NetSquared Local Group

techsoup

Acclivity

Adobe

Alpha Software

Atlas Business Solutions

Atomic Training

Amazon Web Services

Autodesk

Azavea

BetterWorld

Bitdefender

Blackbaud

Bloomerang

Box

Brocade

Bytes of Learning

Caspio

CauseVox

CDI Computer Dealers

Cisco

Citrix

CitySoft

CleverReach

ClickTime

Closerware

Comodo

Connect2Give

Dell

Dharma Merchant Services

Digital Wish

Dolby

DonorPerfect

DocuSign

Efficient Elements

FileMaker

GoDaddy

GrantStation

Guide By Cell

Headsets.com

Horizon DataSys

HR Solutions Partners

Huddle

Idealware

InFocus

Informz

InterConnection

Intuit

JourneyEd

Litmos

Little Green Light

Mailshell

Microsoft

Mobile Beacon

NetSuite

Nielsen

NonProfitEasy

O&O Software

Okta

Quickbooks Made Easy

Reading Eggs

ReadyTalk

Red Earth Software

Sage Software

Shopify

Simple Charity Registration

Skillsoft

Smart Business Savings

Society for Nonprofit Organizations

Sparrow Mobile

Symantec

Tableau

TechBridge

Tech Impact

Teespring

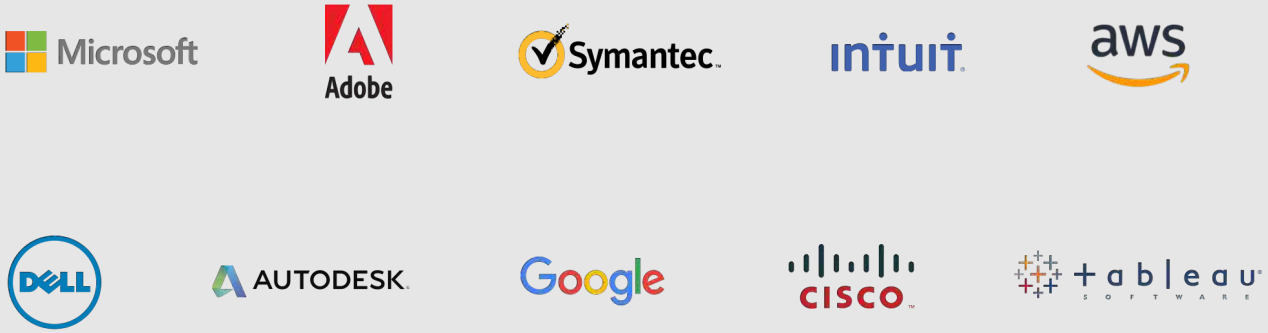
Telosa

Tint

Ultralingua

Western Digital

Zoner



Explore our Nonprofit Tech Marketplace

"We are an all-volunteer organization with limited professional skills. Adobe's donated technology is helping us present our story to the public and to lenders in the format of a much larger organization. With Adobe, we are able to knock off a few of the "rough edges" so that our story is front and center instead of our technological limitations. Thank you, Adobe!"

- **Richard de Koster**
  Constitution Island Association, Inc

For more information, please visit
www.techsoup.org/get-product-donations

Presenters

Michael Enos
Senior Director of Community and Platform
TechSoup

Sima Thakkar
Online Learning Producer
TechSoup

Assisting with chat:
Zerreen Kazi
Marketing Associate
TechSoup

Michael Enos
Senior Director
Community and Platform
TechSoup

Sima Thakkar
Senior Manager, Content
TechSoup

Zerreen Kazi
Marketing Associate
TechSoup

Agenda

Introduction: Why is it important to be safe online?

Tip 1: Make it more difficult for hackers
Tip 2: Establish policies for staff and volunteers
Tip 3: Deter deceit
Tip 4: Secure mobile devices and remote workstations
Tip 5: Be vigilant when you use public computers
Tip 6: Be cautious when you use public Wi-Fi
Tip 7: Social media is social (not "private")
Tip 8: Limit how much you share
Tip 9: Be careful when your organization uses social media
Tip 10: Exercise caution with logins and consider whether to limit access to shared files
Tip 11: Familiarize yourself with the cloud provider's policies
Tip 12: Keep offline backups

Tip 1: Make it more difficult for hackers

- Be smart about passwords
  - Use different passwords for different websites
  - Use two-factor authentication whenever possible
- Keep your software up-to-date
- Security updates and Anti-virus definitions
- Use a spam blocker

Tip 2: Deter deceit

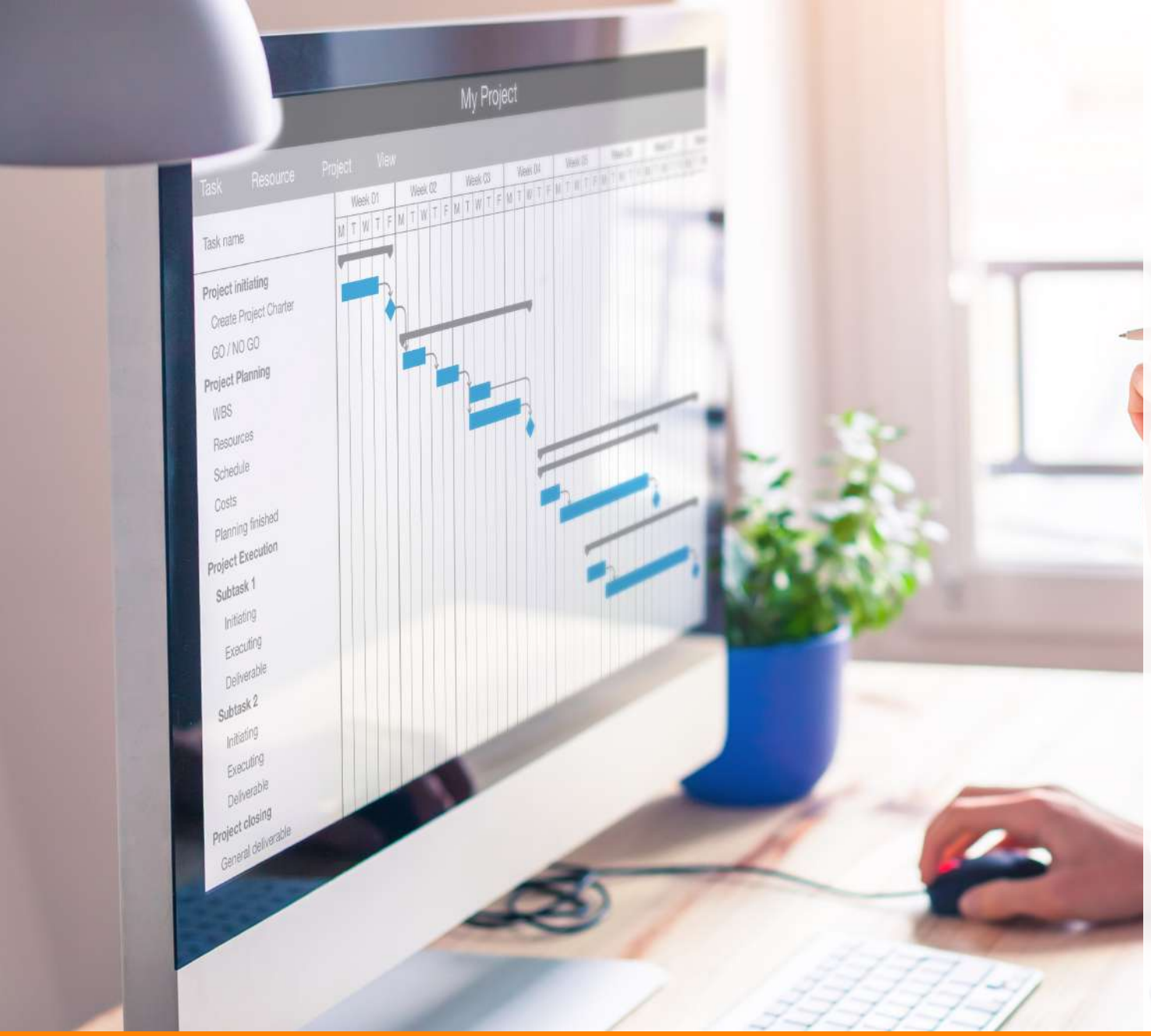
- Avoid social engineering
  - Never provide your password or other sensitive information!
- Beware of ransomware
  - Designed to defraud unsuspecting users. It convinces you that your device is infected with a computer
- Browse the Internet more securely
  - Check for the https: in the URL and that the certificate is up-to-date

Tip 3: Establish policies for staff and volunteers

- Develop a cyber-security awareness training program
  - Mandatory for all staff and others who access your organizations systems and data
- Establish an acceptable use policy for computers and mobile devices
- Use single sign-on wherever possible, or an identity management service such Microsoft ADFS or Okta

Tip 4: Secure mobile devices and remote workstations

- A mobile device should never be the only location for any set of important data
- Restrict access to your device with a PIN or password
- Use encryption on mobile devices for any sensitive data



Tip 5: Be vigilant when you use public computers

- You should view every public computer as a security risk
- In a public space, you also need to be particularly aware of physical security
- Never insert your devices or drives into a public computer
- Be aware of who might be viewing your screen

Tip 6: Be cautious when you use public Wi-Fi

- You should treat all public Wi-Fi networks as insecure
- Use your cell phone as a mobile hotspot
- Use VPN if you can when on a public network

Tip 7: Social media is social (not "private")

- Anything you post online is both permanent and transmittable
- Social media is a popular entry point for phishing and social engineering
- Consider your company's Code of Conduct

Tip 8: Limit how much you share

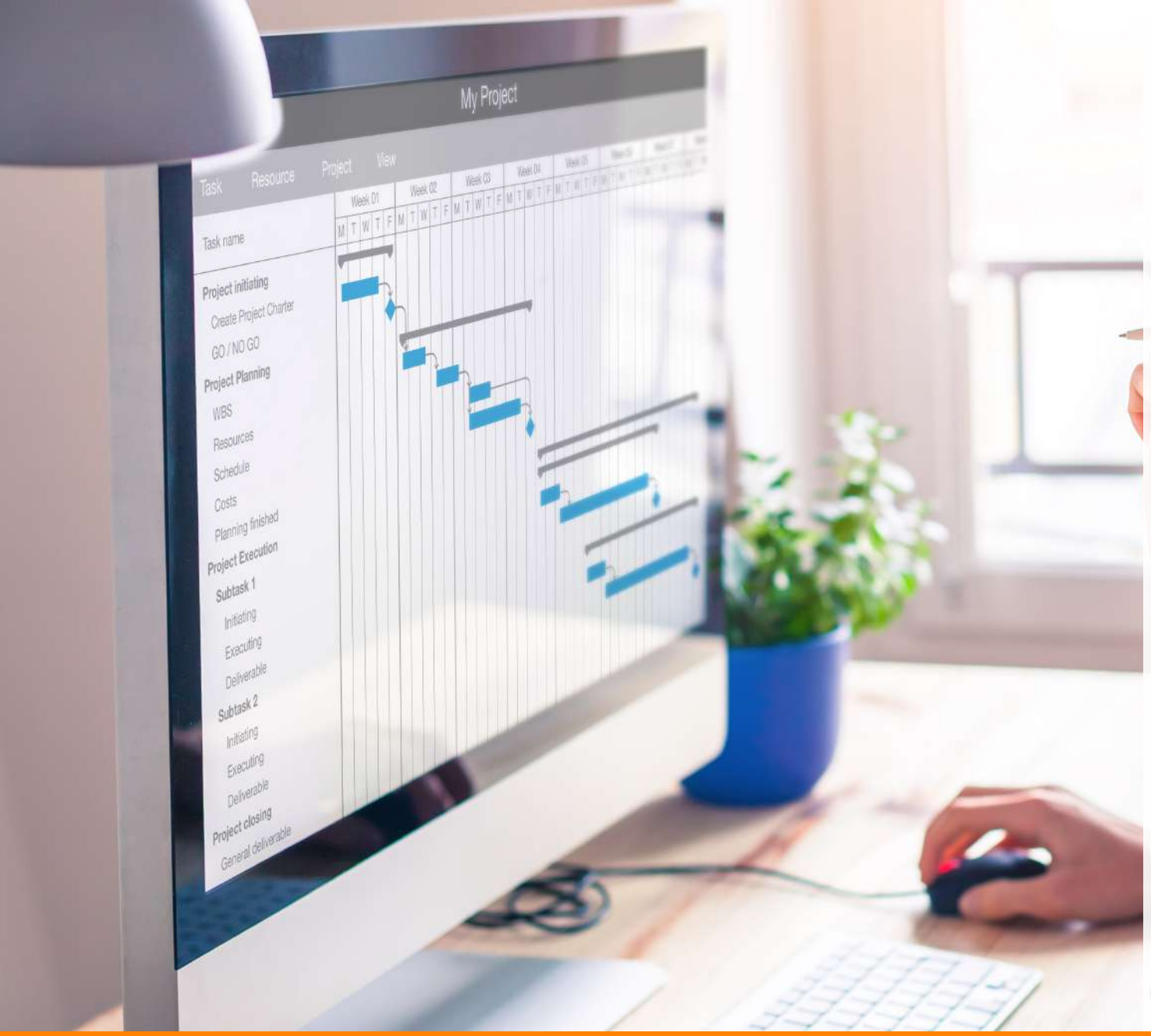
- Personal details can be used to defraud, impersonate, or find you
- Post only things that you would be comfortable to be heard in public
- Use common sense!

Tip 9: Be careful when your organization uses social media

- Special care must be taken when staff and volunteers use social media on behalf of the organization
- You should have a social media policy in place for your organization, if not, create one!
- Assign roles to staff as appropriate

Tip 10: Exercise caution with logins and limit access to shared files

- Each staff member or volunteer should have a unique login
- Employ two-factor authentication when possible
- Establish clear policies and security controls around file sharing



Tip 11: Familiarize yourself with a cloud provider's policies

- Be aware of the provider's policies in terms of data ownership and residency
- If authorities request your data, the service provider will likely comply and give your data to them
- Consider the importance of maintaining control of your data if appropriate

Tip 12: Keep offline backups when appropriate

- Consider data that you want to put in the cloud, and how the inaccessibility of that information would affect your organization's ability to operate

- If you are backing up data from the cloud, make sure it is encrypted

Questions?

techsoup

Share and Learn

- Chat in one thing that you learned in today's webinar.
- Please complete our post-event survey. Your feedback really helps.
- Follow TechSoup on social media (FB, Instagram, Twitter)
- Visit the TechSoup Blog at blog.techsoup.org

Join us for our upcoming webinars.

10/22
Microsoft in the Cloud: Making Migration Easy

10/25
Is the Cloud Safe? Ensuring Safety in the Cloud

10/29
How to Convert Community Stakeholders to Impact Investors

10/30
What Open Source Is and How Your Nonprofit Can Benefit

Archived Webinars:
www.techsoup.org/community-events

techsoup

Thank you to our webinar sponsor!

Please complete the post-event survey that will pop up once you close this window.