PROTECTING THE GREATER GOOD | Church Mutual INSURANCE

TOP 5 COVID-19 CYBERSCAM WARNING SIGNS

We've all felt intimidated and stressed about learning new technology and platforms. Now COVID-19 is making it a must for you and members of your community to carry out your organization's operations and routines virtually. As you engage with more digital services and platforms during this unprecedented time, keep these tips in mind to reduce the risk of cyberscams and data breaches that are more likely to occur during a pandemic.

WARNING SIGN #1: RECEIVING PANDEMIC-RELATED EMAILS AND ATTACHMENTS

Hackers are taking advantage of the fear and uncertainty the world is feeling. They are using phishing tactics to try to breach your data, posing as a reliable source providing information about stimulus checks, unemployment benefits and charitable information around coronavirus relief.

CYBERSAFETY TIPS

✓ Do not click on links from suspicious email senders. Rest assured, governmental officials will not send unsolicited emails seeking private information in order to send money

✓ Ignore emails around COVID-19 that include multiple typos and grammar errors

✓ Not all charity and donation pages are for legitimate organizations. Beware of those asking for gift cards or wiring payments – those are usually scams

WARNING SIGN #2: DOWNLOADING AND RUNNING A NEW APPLICATION DURING A CRISIS

A common way for criminals to access data is by prompting users to download a new application related to COVID-19 that contains malicious spyware

CYBERSAFETY TIPS

✓ Double-check the credentials of any application before downloading

✓ Turn off any "automatically download" features of email and other communication tools

✓ If you have any doubt whatsoever, do not download the application

WARNING SIGN #3: UNSECURED SMART HOME DEVICES

During the pandemic, working from home is likely leading you to mix work and personal online usage. Hackers may try to access important data by connecting through your home's smart devices.

CYBERSAFETY TIPS

✓ Secure your home's Wi-Fi access point with a new password and limit the devices you allow to connect

✓ Connect to your organization's virtual private network (VPN) to create a trusted internet connection between you and your organization

✓ Promptly install all updates, including anti-virus software, to all devices while removing any unused apps

WARNING SIGN #4: LOGIN INFO REQUESTS

While working at home during this pandemic, you may receive more requests from your leaders and volunteers to share login information. Most are well-meaning – they want to help you live out your mission online. Be careful when providing that information; hackers are using this opportunity to pose as members of your community to gain login information to breach your data.

CYBERSAFETY TIPS

✓ Update the passwords to your website, portals, profiles and organization's other digital tools every two weeks

✓ Only provide passwords to your leaders via a phone call – never an email

✓ Use two-factor authentication that verifies a person's identity for all internal systems and data

WARNING SIGN #5: UNEXPECTED VISITORS ON YOUR VIDEO CONFERENCE

Screen sharing and virtual meetings are becoming the new norm to organize with leadership and connect with community members. Unfortunately, more people are seeing their video conferences interrupted by unwelcome visitors coming on screen to disrupt a call or try to listen in for valuable information. (Think of it as prank phone calls for the digital age!)

CYBERSAFETY TIPS

✓ Leverage the waiting room feature of video conferencing tools to vet attendees before going live

✓ Prevent unwanted newcomers from joining an existing meeting by requiring a password to enter

✓ Add a limit on screen sharing so only those with permissions can share their screen

It's more important than ever to protect your organization and your people while navigating an online presence amid the coronavirus pandemic. We're here to help you through the virtual challenges. If you have questions around safely serving your community in an online space, please reach out to a Risk Control Team Member at **riskconsulting@churchmutual.com**.

PROTECTING THE GREATER GOOD | Church Mutual INSURANCE

The information contained in these materials is intended solely to provide general information pertaining to the subject matter covered by the sources deemed reliable by Church Mutual to present accurate and reliable information. Church Mutual Insurance Company, S.I. is stock insurer[1] and its affiliates offer insurance and services. Church Mutual does not warrant that these materials are all-inclusive or that they are accurate. The information provided may not constitute the most up-to-date information. Any readers should consult with professional advice prior to relying on any information that may be found in these materials.

[1] Church Mutual is a stock insurer whose policyholders are members of the Church Mutual Insurance Company, S.I. Group. 2020-21-0000 (Rev. 04/20)