Evangelical Lutheran Church in America
God's work. Our hands.

Information Security Webinar Questions and Answers

Contents

Email Security

"Email spoofing is the creation of email messages with a forged sender address." – Wikipedia. You may receive messages that appear to be the sender asking you to do something for them, usually with some urgency to the request. It's not really the sender. What can you do to prevent this? Is there anywhere spoofing can be reported?

> *In addition to End User Information Security Awareness, the ELCA recommends not using "free" personal email accounts for synod and congregation church communications and business. ELCA synods and congregations are eligible for Microsoft Productivity Solutions for Nonprofits at no-cost or minimal cost for Microsoft Advanced Threat Protection with more advanced security features to protect against email spoofing and phishing.*
>
> *Click here for more information on Microsoft Productivity Solutions for Nonprofits.*
> *Click here for more information on Microsoft Advanced Threat Protection.*

What are your recommendations for encrypting and securing email and other data when you're using free accounts from services such as Google and Yahoo?

> *If you are using recent versions of Microsoft Office products such as Word, Excel and PowerPoint, you can natively encrypt the document with a password by selecting Info – Protect Document – Encrypt with Password.*
>
> *For other files, you can leverage WinZip for file compression and encryption with a password.*
>
> *Click here for more information on* **WinZip**.
>
> *Be sure to use a complex password with a phrase and mix of characters.*

My email has been spoofed three times in the last four months. How do they get my contact list?

> *An attacker attempting to impersonate your email address with look-alike domains using similar characters does not have access to your email or contact list. But if your actual email account is compromised in terms of the attacker was able to obtain your password from it either being easily guessed or from a list for sale on the dark web, they have access to your email and contact information. If you believe your email account has been taken over, change the password to a complex one, or if the attacker has already changed and locked you out, contact your email service provider to report the security incident and ask for instructions on how to remediate.*

How are people getting the information they are using for these whaling attacks? What personally do we need to be particularly attentive to?

Attackers leverage public information readily available on the internet either through news media or social media websites and Google searches. The best protection is to not use social media or at least minimize the use of Facebook, Twitter, LinkedIn, Instagram, Snapchat, etc.

Many ministry leaders are member volunteers but do not want to use their personal email accounts for a variety of reasons. What do you recommend for setting up "satellite" accounts? Do you have any policy language that makes it clear these addresses may be shared with others?

The ELCA recommends not using "free" personal email accounts for synod and congregation church communications and business. ELCA synods and congregations are eligible for Microsoft Productivity Solutions for Nonprofits at no-cost or minimal cost for Microsoft Advanced Threat Protection with more advanced security features to protect against email spoofing and phishing.

Click here for more information on Microsoft Productivity Solutions for Nonprofits.

What if a phishing scammer says they "know your password"? They get part of the password right. I report it to phishing, but should I be doing something more?

The majority of these types of phishing attempts are using social engineering techniques to try to get you to believe that they have access to your email account, device, webcam, etc. More than likely, they were able to obtain the "old" or "partial" password from a database of email addresses and passwords available for sale on the dark web. If it is an "old" or "partial" password and not your current password, it is best to mark it as "SPAM" email and change your password to a complex password just to be safe. If it is your actual current password, change your password if you can to a complex password and contact your email service provider to report a security incident and request assistance in addressing the issue.

Online Meetings & Virtual Church Service

You are using Skype. Is it safer than Zoom?

We are using a tool called Skype Broadcast for this webinar, a special version of Skype intended for webinars. Zoom has had many well-publicized security risks in recent weeks that have not been resolved. We have advised that people not use Zoom until these security risks are fixed.

I understood passwords and waiting rooms blocked Zoombombing, no?

There are many ways that attackers are taking advantage of Zoom's security weaknesses and lack of default security settings. Besides adding passwords and waiting rooms to be allowed in, it is recommended to:

- *Disable "Join Before Host" so people can't cause trouble before you arrive.*
- *Enable "Co-Host" so you can assign others to help moderate.*
- *Disable "File Transfer" so there's no digital virus sharing.*
- *Disable "Allow Removed Participants to Rejoin" so booted attendees can't slip back in.*

Click here for more information on How to Keep Uninvited Guests out of Your Zoom Event.

You seem really down on Zoom and recommended Skype or Microsoft Teams. If not everyone has Microsoft subscriptions, does that leave Skype as the only option? Isn't Skype owned by Microsoft? Is a multiparty Skype call free?

> *Zoom has grown quickly and added features at the expense of security. Microsoft's tools exist in their highly secure Azure cloud. Microsoft Teams does not require licensing to use. Check out this link or search "Microsoft Teams Free" in a web search tool: https://support.microsoft.com/en-us/office/welcome-to-microsoft-teams-free-6d79a648-6913-4696-9237-ed13de64ae3c?ui=en-us&rs=en-us&ad=us.*

So, it has been a few weeks since the Zoom issues surfaced. At this point, do you still recommend moving from Zoom to Skype?

> *Yes, Zoom has still not addressed all of the security issues that have been identified.*

We have propagated the use of Zoom for group or team meetings in the church. How hard will it be to make changes to Skype?

> *This is highly subjective. It depends on how savvy your users are.*

Did I understand that the ELCA has been advised not to use Zoom technology?

> *Jon Beyer has urged all churchwide staff to avoid using Zoom until they can fix the security vulnerabilities. These vulnerabilities have yet to be fixed.*

We are currently using Zoom. If we started using a VPN, would it make it more secure?

> *Not really. The security issues are with the platform itself. It wouldn't secure the weaknesses in the platform.*

How big is the risk of continuing with Zoom at the moment? And If we decide it is problematic to switch from Zoom at this time, what safety precautions do you recommend we can take?

> *There are many ways that attackers are taking advantage of Zoom's security weaknesses and lack of default security settings. The following safety precautions should be taken when using Zoom:*
>
> - *Add a password to your Zoom session for participants to input before entering the session.*
> - *Enable "Waiting Rooms" to require participants to be let in.*
> - *Disable "Screen Share" for other participants.*
> - *Disable "Join Before Host" so people can't cause trouble before you arrive.*
> - *Enable "Co-Host" so you can assign others to help moderate.*
> - *Disable "File Transfer" so there's no digital virus sharing.*
> - *Disable "Allow Removed Participants to Rejoin" so booted attendees can't slip back in.*
>
> *Click here for more information on* How to Keep Uninvited Guests out of Your Zoom Event.

Is there a more secure program other than Zoom for meetings?

> *Skype for Business, Microsoft Teams and WebEx are more secure today than Zoom. Zoom has several outstanding security issues as of April 27, and that is why we don't recommend using it. ELCA synods and congregations are eligible for Microsoft Productivity Solutions such as Teams Web Collaboration for Nonprofits at no-cost.*
> *Click here for more information on Microsoft Productivity Solutions for Nonprofits.*

We have been using Zoom for worship. Does Skype work in the same way? It is hard for some of our older members to figure this out.

> *All online gathering software works in a similar way. They differ in back-end technology, features offered and interface design. No matter what software you use, it's important to practice using it before your live event so you're ready to lead a successful event. External participants will want to install the software ahead of the event and, if possible, join a practice event too.*

Staying Safe While Browsing the Web

Can you be confident to close a pop-up window using the X in the corner of the pop-up window? Couldn't that be the "click" that they want you to do?

> *You can close a pop-up with the X in the corner of the window, but you need to be careful that you're clicking the outermost X and not something inside of the window. Closing the browser window will not be the "click."*

Our church website is secure (HTTPS), however browsers still say the site is unsecure. Is that a question for our hosting service provider?

> *Yes, you should be in contact with your hosting service. Good question.*

I see the "In-Private" windows on the browsers. Is that as safe as it sounds?

> *It prevents tracking cookies, but all browsing is still at the mercy of the user behind the keyboard.*

What are internet guidelines when you are working from home and the computer is for both work and personal use?

> *It is recommended that personal use not be conducted on company-provided devices and company work-related tasks not be performed on personal devices. If unavoidable, ensure that a strong Endpoint Protection Platform or Anti-Virus software such as Microsoft Windows Defender or Cylance is being utilized and working properly to protect both work and personal information. In addition, extra precautions must be taken to not open attachments in email, click on web links or download software with malware that threatens your personal and work information.*

Our church's Facebook page address doesn't start with HTTPS. Is this secure and correct?

If you are accessing Facebook with a web browser such as Microsoft Edge, Google Chrome or Apple Safari, you should be seeing https://www.facebook.com/. If you are accessing Facebook from a mobile app on your mobile device, then you would not see https:// as this is only a web browser security feature and the mobile app has its own secure encrypted connection that is not visible to the user.

What sort of minimal measures of security should your website have?

Websites should be developed with strong security controls in mind as recommended in the OWASP Top Ten Web Application Security Risks.

Click here for more information on OWASP Top Ten Application Security Risks.

We used to post our newsletter on our website, which often had emails listed for contact, and figured people seemed to be "scrapping" data from the newsletters (pdfs). Took them down. Is there a way to post newsletters securely?

Rather than posting newsletters with information that attackers could use against your organization, it would be best to email the newsletter PDF directly to the intended audience.

Social Media

What steps can we take to get our Facebook page back from a disgruntled member who is holding it hostage and has recently made changes to that page, then used it to send a friend request?

You might find this link useful: https://www.facebook.com/help/1216349518398524.
Use the first link under Hacked Accounts to work within Facebook's tools.

How safe is putting a donation button on our website and/or Facebook page?

A link to a donation button is as safe as making a purchase from an online retailer. The online giving provider must be Payment Card Industry (PCI) certified. In addition, ensure that the online giving provider is using website security best practices, such as HTTPS, and a CAPTCHA means to validate that the donor is a human.

Click here for more information on Vanco Security.

Click her for more information on Tithe.ly Security.

What's a safe way to vet new Facebook followers for church worship when you want to grow membership?

Vetting new members should include having them provide an email address and phone number to have a discussion and validate their true intentions and prove they are not a cyberattacker. In

addition, reviewing their profile and identifying if any of their friends are also members may assist in the process.

Password Vaults

Password vaults store your passwords securely. Just as important, they enable strong unique passwords for every account. Generally, password vaults require a passcode or phrase to unlock the vault and access all of your accounts. You remember one password – the vault remembers the rest.

Do you have password vaults you recommend?

Reputable Password Vault software includes Keeper, LastPass and 1Password.

Click here for more information on Password Managers from SANS OUCH Newsletter.

Other Software Questions

A photo-editing program I downloaded to the church's main computer had a web address beginning with https. Does the S indicate the site is safe? I checked online to see how the site was evaluated, not only for performance, but for reliability and safety. Did I do enough due diligence?

Good question. Websites that use https are more secure than those that are only http, but it does not guarantee that the site is safe. While there are lots of "free" software options out there, you do take risks using free versions from companies with which you are not familiar. It's tough to determine [if you've done sufficient diligence without more information]. It would be good to find a local tech-savvy person to help ensure you've selected a safe software.

If you have a firewall and MS Windows Essentials, how much more anti-virus, etc. is needed? Our IT vendor claims this is enough.

This is likely enough as long as it is Microsoft Security Essentials.

What software do you recommend for screen saver protection?

None – set the lock screen to lock in 5 minutes or less and require a password to log back in.

Also how do you suggest protecting our routers/LAN?

For network hardware, we recommend keeping the firmware up to date and changing the default administrator password.

Is Malwarebytes a reliable/good product to run for spam/phishing?

Malwarebytes is an anti-virus tool that will protect your computer from malicious software that can take over your computer. Solutions for spam and phishing attacks include Microsoft Advanced Threat Protection, Proofpoint and Mimecast.

If we buy Office 365 for our church office, how could we get our own domain/email accounts?

Microsoft Office 365 allows you to obtain your own domain for email accounts when you sign up for the service.

What security package, if any, is recommended for the church to be using? Norton? McAfee, etc.?

Recommended Endpoint Protection Platform or anti-virus software includes Microsoft Windows Defender, Cylance, Norton or McAfee.

Where do you store backup information rather than on a flash drive?

We recommend subscribing to a file sharing or backup service such as Microsoft OneDrive, Citrix ShareFile or Dropbox.

What is the name of the antivirus software Chris mentioned?

Recommended Endpoint Protection Platform or anti-virus software includes Microsoft Windows Defender, Cylance, Norton or McAfee.

Do you recommend Dropbox as a backup?

We recommend subscribing to a file sharing or backup service such as Microsoft OneDrive, Citrix ShareFile or Dropbox.

Phone Calls & Identity

Can you explain the details and techniques related to the suggestion to "Confirm the caller's identity with a PIN or established security questions"?

Before initiating a financial wire transfer, payroll bank account information or other confidential transaction, don't just accept an email request. You should also contact the requester to ensure it is in fact them making the request and not an attacker in a compromised email.

A couple of times in the past year, our pastor's phone has been hacked and texts have gone out asking for gift cards. How do we stop this? We do inform our congregation immediately that he was hacked.

It is best to contact the cellular service provider to report the security breach and investigate the source of the attack. They may be able to monitor or block the hacks or provide a new phone number as a worst-case option to resolve the issue. For example, if you have Verizon Wireless, review their Account Security, Common Frauds and Scams website.

How do I know if my data was breached?

In general, it is difficult to detect breaches without advanced email, endpoint, network and cloud threat detection solutions. Other solutions include monitoring logs and correlating events for anomalies in system behavior behind the scenes that a user is unable to detect themselves.

Also, financial and retail organizations that have elements of your confidential personal information are required by government regulations and industry mandates to publicly report and provide notification to users in the event of a data breach.

Is there a good resource to share with my members to instruct them on how to spot a fake text, phone call, email or Facebook? Elder fraud has been huge in my area lately.

SANS.org provides valuable resources for home cyber security such as Creating a Cyber Secure Home poster.

For more information, read Messaging / Smishing Attacks in the SANS OUCH Newsletter.