Trust but Verify

Defeating Cyber Criminals Before They Break In

One of your pastors is leading a group of volunteers on an overseas mission trip. You receive an urgent email that a volunteer was injured in a terrible accident. The email instructs you to send funds for life-saving medical treatment and provides a link to electronically transfer the money. Sensing the urgency of the situation, you take immediate action. Two hours later, the pastor calls to check in. You ask him about the injured volunteer. After a short pause, he asks, "what injured volunteer?"

Scenarios like this happen all too often. "Scammers use emotion to get people to act quickly to solve or prevent a seemingly serious issue – medical emergencies, late payments on a critical service like internet or utilities, even ransom payments for team members traveling abroad," shared Matt Cohee, a network security analyst with Brotherhood Mutual. The technique is called social engineering, and the goal is simple – to get you to act before you have time to think. The result can be stolen funds, stolen information, or ransomware placed on your computer network, any of which can tie up your organization's resources or even cripple your operations.

Five Common Tricks of Cyber Scammers

Scammers use many schemes when attempting to steal your data, but you can outsmart them by understanding their methods.

Phishing emails are one of the most common ways scammers try to get data or gain access to your network. They typically incorporate elements of surprise, scare tactics, or fear of imminent danger.

Spear phishing is a targeted phishing attack that uses personalization in the email to make it appear legitimate. Hackers may even use information from your organization's website or social media account, or your pastor or head of school's social media account, to craft an email specific to your church, school, or camp.

Spoofing imitates an email address or website to make you think you're interacting with someone you know and trust. Hackers typically change one letter and hope you won't notice. An example email address could be: pastor@dtchurch.org (real) and pastor@dtchurch.com (fake). Once they gain your trust, they can lead you to download malicious software, release funds, or disclose sensitive information.

Vishing and Smishing are another form of phishing. The scammer uses phone calls or text messages instead of emails.

Pretexting creates a story in order to gain your trust. The story, or pretext, uses trust to manipulate you into thinking the scammer is legitimate. For example, someone might impersonate a vendor you typically use to gain access to your building or computer systems.

Secure Systems and Data

1. Avoid using personal accounts for ministry activities.
2. Avoid emailing sensitive data and make sure it is only accessible to those who need it.
3. Make sure you can access password protected data if someone leaves the church or vacates a position. Change passwords to secure the account.
4. Keep the software on your smartphones and computers up to date so you have the latest security patches.

Outsmart the Hackers

Scammers can be very sneaky, which makes it difficult to spot their tricks. Managing passwords and using two-factor authentication are just two ways you can outsmart their treachery.

Manage Your Passwords

Passwords help protect systems and data from unwanted access, but they can create a false sense of security. With so many separate accounts that require passwords, it's common for people to use the same password across multiple systems and accounts. "Hackers are constantly trying to steal your passwords. If they steal one, and you use it everywhere, they now have access to all the accounts that use the same password," said Chris Harvey, chief information security officer with Brotherhood Mutual. A simple remedy is to use a password manager. It comes as software and an app so you can use it across your computers and mobile devices. Password managers allow you to place all your accounts in a single, encrypted and password-protected vault. Once you link your accounts, the software creates new, unique passwords for each. You'll only need to remember the single master password. Cohee advises, "With passwords, the length is really the difference. Make sure it's complex, and it could even be a sentence, which is even more secure."

Two-Factor Authentication

Two-factor authentication takes security to a new level. It requires users to have a password and an additional method of verification, such as a pin number, texted to a smartphone, before they can gain access to an account. This is a very effective way of securing your accounts. "If an account offers two-factor authentication, use it," encouraged Harvey. This type of security places an additional step to gain access to accounts. This means that even if your password is stolen, hackers won't be able to access your account because they won't have access to the pin on your smartphone.

Think Before You Click

Whenever you receive an email, text message, or phone call that requests immediate action, especially a transfer of funds, take a minute to run through the following questions:

- Were you expecting it?
- Is it a known problem that you need to address?
- Did you receive an email when a phone call or in-person conversation would have been more appropriate?

To add an additional layer of protection, check any hyperlink before clicking it by hovering your cursor over the link. “If it looks strange or contains misspellings, simply avoid clicking,” cautioned Cohee. “And if you get a text message asking you to call a phone number for a business, such as a bank, always do an online search and call the listed number so you know it’s legitimate.”

When a company experiences a cyber breach, it can expose your username and password.

If you use the same password everywhere, hackers will use software to automatically search other accounts and attempt to break in with the stolen password, which is called **password stuffing**. They can even get into your email account and send emails on your behalf, essentially using ministry email to attack other businesses or people.

1. Avoid using personal accounts for ministry activities.
2. Avoid emailing sensitive data and make sure it is only accessible to those who need it.
3. Make sure you can access password protected data if someone leaves the church or vacates a position. Change passwords to secure the account.
4. Keep the software on your smartphones and computers up to date so you have the latest security patches.

Cybersecurity Coverage

While theft through email phishing scams may be covered under your ministry’s theft coverage, losses from many types of cyber threats are not. Should a breach occur, your ministry could have costs associated with required notifications, credit monitoring services, and data retrieval for litigation. Brotherhood Mutual offers multiple coverage options* for cyber liability, as well as a partnership with a global leader in cyber response and remediation services. If a breach exposes personally identifiable information, remediation services help fulfill legal requirements to report the hack to those potentially affected. Kevin Rainear, senior claims adjuster, Brotherhood Mutual, advises to alert your insurance agent first if you have a cyber incident. “If there’s concern personal information stored on your systems has been compromised, the breach response services provided with Brotherhood Mutual’s cyber liability coverage may help your ministry investigate the breach and determine if there is a legal obligation to report to those who may be impacted,” said Rainear.