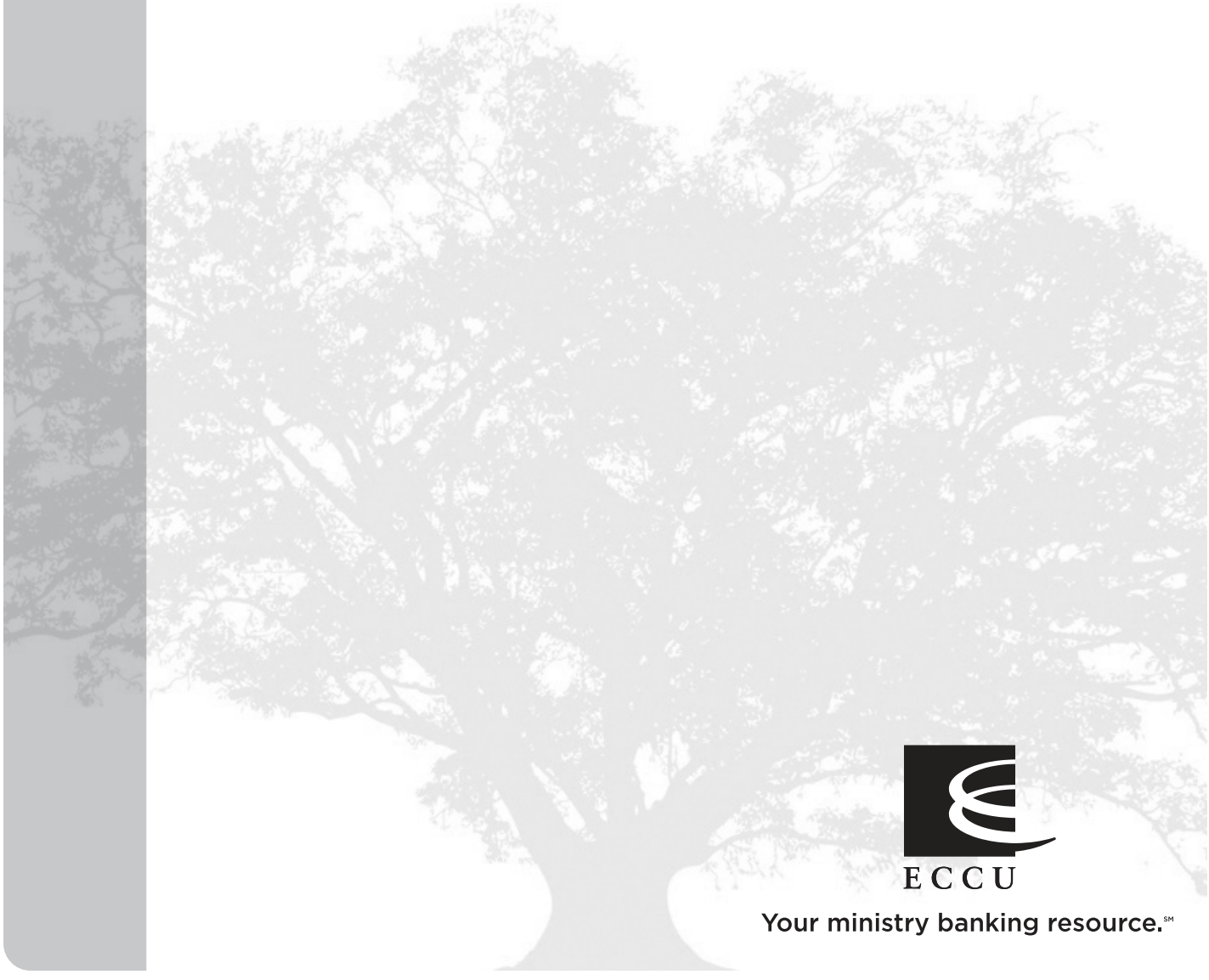
Is your data secure?



ECCU

Your ministry banking resource.℠

You're not as safe as you think

Think for a moment: Where do you keep information about your congregants or donors? In an Excel file on someone's desktop computer? An Access database housed on your laptop? If someone were to steal your computer, would she suddenly have the names, phone numbers, and addresses of your givers at her fingertips? If a hacker wormed his way into your desktop, would he find information about people's giving, including checking account numbers? Keeping your congregants' and donors' personal information secure is more than a matter of integrity; it's a legal matter as well.

What about your ministry's financial and banking information? Where is that kept? Are you vulnerable to outsiders' accessing and abusing ministry funds?

It's becoming increasingly easy for personal and financial information to be accessed as more and more churches utilize 21st century technology. So the question arises: How do you prevent your ministry's information from being abused by those with malicious intent?

Common gateways

E-mail has become the most prevalent form of business and personal written communication. Its popularity, however, is now one of its liabilities, increasing its vulnerability to attacks from hackers.

Different ways hackers use e-mail to attack

E-mail formatting

Special effects in text and graphics are created using a programming language called HTML. These enhancements are vulnerable to malicious program code that recipients will never see. Since harmful code is usually HTML, the simplest way to eliminate vulnerability is to eliminate HTML. There are two ways to do this safely:

1) *Turn off HTML preview or formatting*. E-mail preview feature automatically displays the contents of a message once the e-mail is selected. The issue arises when you select a suspicious e-mail intending to delete it. As soon as the e-mail is selected, the malicious code is run.

2) *Turn off HTML formatting completely*. This will eliminate the risk but will also prevent legitimate e-mails that use HTML from being read correctly.

It is also recommended that you regularly upgrade to your email provider's latest updates to make certain you have the most effective barrier to malicious code.

E-mail attachments

Opening e-mail attachments can also execute harmful code. Many times these attachments have nondescript names or are documents that were never requested. These attachments will not infect a computer unless they are opened. *E-mails that contain unsolicited attachments should be deleted without opening them.*

Web based e-mail

Web-based e-mail gives users access to e-mail from any computer on the Internet, making it convenient for those people who travel extensively to communicate with colleagues and friends while away. Web-based e-mail uses HTML programming language to generate the graphics that users see, so it is susceptible to malicious coding that can cause damage to a computer system.

Secure connections - By default, Internet web-based e-mail services ask for a username on a page that is not encrypted. Sending a username and password over the Internet is like sending a letter with a home address on it and taping the house key on the outside of the envelope. Not only are you letting people know where your e-mail account is located, but you are also giving away the key to access it.

To remedy this problem, most web-based e-mail providers offer secured communications in the form of SSL. SSL Internet traffic is encrypted and virtually impossible to read in transit. A small lock symbol will appear in the status bar of the browser when communication is being sent securely.

Spam

Spam e-mail can be coded to track when a user views an e-mail offer, which lets the sender know that a valid e-mail address has been found and that the user will view spam e-mail. This information is then sold to list providers who in turn sell it to other spam companies. The e-mail address is then flooded with numerous offers for products and services.

Phishing

Phishing attempts to capture personal information by sending e-mails that ask users to update their information. Often these e-mails appear to come from an organization with which the user has a relationship; a hyperlink within the e-mail shows the organization's real website. However, the website to which the hyperlink sends the user does not actually match the web address listed in the e-mail. *Always verify that the website address to which you have been directed matches where you thought you were going.*

Other areas of vulnerability

Web surfing

"Surfing the web" can present many hazards that seem benign but prove to be either annoying or destructive.

Malicious Code - Web pages are created using programming languages that provide the robust and dynamic viewing experience that has made the Internet so popular. However, this programming also allows criminals to take advantage of some of the flaws in your computer.

Vulnerabilities in computer systems allow hackers to code their web pages with instructions to install programs that will send personal information back to the hacker or, in some cases, will allow a remote hacker to take control of a computer. *The best way to avoid falling victim to these criminals is to only visit sites of reputable companies, and never enter or divulge personal information through a website unless you are familiar with the company and what it will do with the information.*

Pharming

Pharming, while similar to phishing, is one of the more difficult attacks to detect. The hacker attempts to send a user to a non-legitimate website in order to collect the user's personal information. However, in pharming, the website address looks just like the legitimate website address. The difference is in the code, which the casual web surfer doesn't usually notice. For example, you might click on a link that looks like www.eccu.org, but in the code is actually www.eccug.org. You're then sent to a non-legitimate website.

The best defense against this type of attack is to only enter personal information when the address matches the intended address and the site is securely encrypted with a valid certificate. To view the certificate, double click the lock symbol at the bottom of the browser. The dialogue box that appears should list the intended company, and no warnings should appear.

Chat rooms and bulletin boards

Chat rooms and bulletin boards enable users to share ideas, opinions, and other information. Posted information is generally archived so that others may review it later. Internet search engines such as Google and Yahoo index these postings so they may be retrieved from their respective websites. Criminals will use this information to build profiles on victims. From the posted information, they can usually find names, addresses, phone numbers, family member names, employer information, e-mail addresses, and more.

Personal information should never be posted in a chat room or bulletin board. It is also recommended that users sign up for and use an e-mail account at a free service when posting to these forums. This will lessen the likelihood of spam e-mail being sent to a work or personal e-mail address.

First line of defense

Firewalls

Hackers actively search for vulnerabilities in computer systems connected to the Internet. A firewall will help prevent unwanted access to a computer or network. Metaphorically, a firewall is the same as locked doors and windows on a house.

A firewall can be an application that is installed on the computer system or a device that sits between the computer system and the Internet. In either case, the function is the same—to protect information from unwanted access. *A firewall is the first line of defense against unwanted attacks on computers. If a computer is going to connect to the Internet, a firewall is most strongly recommended.*

If businesses or institutions maintain records of customers or members and do not have technical resources to install, configure, and maintain a firewall, they should enlist the services of companies who offer this service. Recent legislation puts a great deal of responsibility and liability on the custodians of these records. (See *Best Practices* section for more information regarding firewalls.)

Keeping the bugs away

Antivirus Software

Antivirus software can be installed to prevent harmful code from running on a computer system. This software scans files, e-mails, and attachments for any harmful code. If it detects harmful code, it can be configured to respond with the following actions:

- *Clean* - This action will remove the offending program code but preserve the contents of the file.
- *Delete* - This action will delete the offending file.
- *Quarantine* - This action will move the file to a special holding bin until the user determines the next action to take and will prevent the harmful code from affecting the computer system.
- *Leave Alone* - The file is left alone, allowing a potentially dangerous file to infect a computer system.

These parameters are configured within the antivirus software program.

Antivirus programs can only prevent malicious program codes they know about. These programs keep lists of malicious program code in definition files. The makers of antivirus programs regularly update these definition files to include new threats. The frequency of these updates varies depending on the program. *For this reason, it is important to install a well-supported antivirus software program*. (See *Best Practices* section for more information regarding antivirus software.)

Liability Issues

California Senate Bill 1386 (SB1386)

Notoriety of personal information theft prompted passage of legislation in California that places greater liability on companies who choose to store personal information. Senate Bill 1386 became effective in July 2003. It states: "*Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person*."

The law allows individuals whose personal data has been compromised to file a civil suit to recover damages resulting from that compromise.

Gramm-Leach-Bliley (GLB)

At the federal level, the Gramm-Leach-Bliley (GLB) Act attempts to place similar burdens of protection on companies throughout the United States. This law requires companies to protect against unauthorized access and anticipated threats or hazards to security and integrity of personal records. GLB requires that organizations implement systems that will detect, prevent, and respond to attacks, intrusions, and system failures.

Member Loyalty and Trust

Violation of these laws can spell financial ruin for a church or ministry trying to defend itself against a suit. Even if an organization survives a lawsuit, it may find itself facing an even bigger hurdle—loss of the loyalty and trust of congregants or donors. A non-profit charitable organization may find it difficult to solicit financial donations if potential donors are concerned that their financial information will be compromised.

Best Practices

End User Security

The best prevention against a computer virus is to not invite it into your system. Train users on e-mail best practices including:

- Deleting e-mails from unknown users
- Not previewing e-mail messages
- Not opening attachments
- Not running macros in documents if they do not know what the macro is doing

System Security

System security efforts should be placed in three categories—prevention (patch management and personal firewalls), detection (antivirus software), and eradication (antivirus software).

Prevention

As stated above, a firewall is designed to prevent unwanted and harmful Internet traffic from reaching the user's computer system. Firewalls are either software or hardware based.

- Software firewalls, sometimes referred to as "personal firewalls," are programs that examine all the communication entering or attempting to enter a computer system. This is the most widely used type of firewall for personal use. It's convenient for users who travel because it runs on the system itself. The downside of a software firewall is that it could slow down a computer system.
- Hardware firewalls protect an entire network of computers and servers. They are usually dedicated systems that are the first point of contact for Internet traffic entering an organization. A hardware firewall can be optimized to process communication very quickly and discard potentially harmful traffic without much delay. The downside of hardware firewalls is that they do not protect mobile systems when they leave their networks.

Detection

If a malicious program such as a worm gets through a firewall, the next line of defense is a good antivirus system, which prevents the spreading of harmful programs once they are on the computer system. Antivirus programs

protect through real-time scanning or manually configured scans through preconfigured responses. Please note that some applications require real-time protection to be turned on.

An administrator or computer owner can configure an antivirus program to either clean, quarantine, leave alone, or delete the infected file.

- *Clean* - the antivirus attempts to rid the infected file of the virus.
- *Leave Alone* - No action taken. The virus files are still there and able to do damage
- *Quarantine* - isolates the file so that it does not infect the computer but can be reviewed later. Selecting quarantine after unsuccessfully attempting to clean a file allows antivirus vendors to create updates to their programs so they can clean those files in the future.
- *Delete* - some viruses are programmed to prevent cleaning or quarantining. In these cases, a system should be configured to delete any file that has a reference to the virus.

In real-time scans, files and e-mails are examined as they are transferred to the computer. If a virus is detected during the transfer the appropriate action will be taken.

Eradication

The ability to safely delete any virus or worm that enters a computer or network is extremely important. If protection systems cannot completely remove harmful programs, steps must be taken to lessen the impact of lost data and limit the risk of information theft.

Loss Prevention

If a virus cannot be removed from a computer system, best practice suggests that the system should be reinstalled. To prevent loss of critical information files, regular back-ups should be taken of the system. Although this will not completely restore all the files, it does provide a safeguard against losing all information.

We have access to wonderful technology that makes our lives easier in many ways. Unfortunately, some technology also allows those with malicious intent to access information that has historically been considered secure. While we can't prevent people from attempting to access personal or financial information about our congregants, donors, ministries, or churches, we must take steps to minimize exposure to such attacks.

Definitions

Application

Employs the capabilities of a computer directly to a task that the user wishes to perform.

Certificate

Generally refers to a digital identity certificate that can uniquely identify a computer system or user.

E-mail

Electronic mail, abbreviated email or e-mail, is a method of composing, sending, and receiving messages over electronic communication systems.

Encrypt

Encryption is the process of obscuring information to make it unreadable without special knowledge.

Firewall

A firewall is a piece of hardware and/or software which functions in a network environment to prevent some communications forbidden by the security policy, analogous to the function of firewalls in building construction.

Hacker

Hackers are people proficient in computers who employ a tactical, rather than strategic, approach to computer programming, administration, or security, as well as their culture.

HTML

In computing, HyperText Markup Language (HTML) is designed for the creation of web pages and other information that are viewable in a browser. HTML is used to structure information—denoting certain text as headings, paragraphs, lists and so on—and can be used to define the semantics of a document.

Hyperlink

A link in a hypertext document to another document or other resource.

Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs users to visit a bogus website where they are asked to update personal information, such as passwords and credit card, Social Security, and bank account numbers that the legitimate organization already has.

Pharming

A technique used to obtain personal and private information by compromising the server that directs the user's Internet requests. Requests to visit a website will be redirected to a website similar to the legitimate site where a user will enter personal information.

Spam

Unsolicited e-mail.

Trojan

A malicious program that is disguised as legitimate software.

URL

A Uniform Resource Locator, (URL, spelled out as an acronym, not pronounced as 'earl'), or web address, is a standardized address name layout for resources (such as documents or images) on the Internet (or elsewhere).

Virus

A self-replicating computer program that spreads by inserting copies of itself into other executable code or documents.

Worm

A self-replicating computer program, similar to a virus, that is self-contained and does not need to be part of another program to propagate itself.

For additional information or resources on this or other banking-related topics, please contact Ministry Resources at 800.634.3228, ext. 1472.