BNUG 2019 05-07 Message in a Bottle—Sending it Safely

The international email system was originally designed for scientists to tell each other jokes and share favorite movies in the middle of the night, while they shared computer time at universities. We're using the same design today to communicate about lawsuits, tax preparation, and our love lives. We need to take serious measures to make sure our private information stays private when we send it to each other. In this spirited discussion, we'll explore a range of methods to do so. Please bring your privacy challenges and the tools you use to work with them. Among the methods we'll discuss are pdf encryption, file sending programs and their hazards, one-way vs. two way secure messaging, how safe is Google and Dropbox, how do we deal with HIPAA and 201CMR17?, winzip encryption, secure and less-secure portals.

Send it safely

A discussion about keeping your communication private

Why email alone isn't safe

- transit
- spoofing
- password hacking
- lockout
- people messing

How to do better:

paid email account

google takeout

SSL

But none this lets you send email safely

To do so , you need encryption

Industry-standard encryption-- AES-256 or AES-128

But the recipient has to be able to decrypt

Single-document solution: encrypted pdfs

-- Mac and newer versions of Office, Quickbooks etc. do this natively

-- pdffill free tools

Winzip

-- great for file packages

-- lets you sort by size across all directories

-- lets you access all files with one password entry

-- compresses the files into one file, saving space and saving lots of time

-- batch file is great, but some work to set up and password is in the clear

7-zip does the basics and is free

Portals-- the password problem

Demonstration: sendthisfile.com

The problem: sending the link is not secure by itself-- the file needs to be encrypted with a password you give the customer by phone, otherwise if the link falls in the wrong hands, they get the file.

Why faxing is safe

Phishing attacks

good way to teach about this-- a list of examples

Big disaster-- the Podesta leak at the DNC in 2016

Picking a strong password:

dictionary and brute force attacks.

what is safe content?

What is safe length?

How can you effectively communicate the password?

How do you store the password? How do you share it with co-workers?

Keepass

Lastpass

I think it's great! From my own experiences, I would add:

Prepare for the need to convince the recipient of the need for security/encryption. How will you respond to:

- "Geeze, just attach and send it, already!"

- "What's the big deal?"

- "I give you permission, just send it in a plain email." -- I've gotten this more than once from financial professional clients of mine (regarding their own personal

data) for whom I'm pretty sure they'd be in violation of compliance regulations if they did that with any of their client's data!

Free vs. paid solutions: Insisting on "free" will limit your choices. What is this worth to you? Can (or should) you pass the cost along to (or share the cost with) the client?

Consider setting up more than one solution (perhaps over time as needed), since any one method may not work with every client/recipient or situation, for either technical or recalcitrant reasons. :)

Portals: Apart from protecting the link, are they secure to begin with? dropbox.com, box.com, One Drive, Google Drive

Don't forget to ask the recipient whether they might already have a secure portal that the two of you can use.

HIPAA: Google Drive offers a Business Associate Agreement for business customers subject to HIPAA - see https://cloud.google.com/security/compliance/hipaa-compliance for more info

How much private data do you need to send securely?

- small: a couple of sentences, a document under a megabyte, or

- medium: up to around 8 megabytes, my rule-of-thumb limit for email attachments, or

- large: over 8mb, i.e., too big to attach to an email

One-way or two-way?

- Are you always the one sending the secure data to other people, and they don't need to send any secure data back to you? (or what they send back to you won't be electronic, e.g., via fax or 1st class mail) or

- Do you need a secure, electronic two-way method, which means that you need to teach the other person how to do this, and (depending on the system you choose) they may need to spend money on it as well? And, will the two of you use the same encryption password, or two different ones?