Trails End Computer Club

Bulletin for the week of DECEMBER 1, 2013

WEEKLY MEETINGS EACH Wednesday Program or Lesson 9:30 - 10:30 AM **One on One Help** 10:30-? **In the Library**	**SPECIAL INTEREST GROUPS:** If you would like to meet in a small group to discuss special computer related subjects or form a Special Interest Group lets discuss it. Our bulletin is also available on line by visiting tecc.apcug.org and clicking on bulletin.	**Our weekly program or lesson is intended to be of interest to all computer users. Following the program an allotment of time will be available for one on one help to those who want a better understanding of something done during the presentation.**

Upcoming Events

Wednesday DECEMBER 4, 2013 Meeting
9:15 AM Set up your computer
9:30 AM Lesson
10:30 AM One on One help

Phishing (Identity Theft) Now Considered as the #1 Web Threat

by Ira Wilsker
WEBSITES and SOURCES:
http://hosteddocs.ittoolbox.com/Phishing_and_Web_Security_WP_Mar13.pdf
http://resources.idgenterprise.com/original/AST-0102181_EECDatasheet_from_KnowBe4.pdf
https://en.wikipedia.org/wiki/Phishing
http://www.consumer.ftc.gov/features/feature-0014-identity-theft
https://www.annualcreditreport.com

In several past columns, I have warned readers about the various methods and techniques that cyber crooks use in order to steal their identities. According to Wikipedia (en.wikipedia.org/wiki/Phishing), "Phishing is the act of

attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication." While phishing has been around for several years, it has now become the major method of online identity theft; according to the cyber security service Webroot, "Phishing 2.0" (the latest iteration of this type of phishing) is currently the #1 web threat facing computer users.
In the past, it was thought that only inexperienced and unknowing computer users were vulnerable to the original "Phishing 1.0" level of phishing attacks, as these unfortunate users would blindly click on any links in an email, and give personal and credit card information to all who asked. In order to protect these highly vulnerable individuals, as well as other more experienced users, the computing industry has upgraded web browsers and security software with the capability to detect most phishing attempts, and alert the user of the risk, or otherwise stop the phishing attempt in its tracks. Not to be impeded by the security improvements incorporated into newer browsers and security suites, and losing a major source of substantial but illicit revenue, the cyber crooks who profit handsomely by stealing the identities of others have created new and improved Phishing methods referred to by the security industry as "Phishing 2.0." According to Webroot, in discussing Phishing 2.0, "(Phishing 2.0 is) ... a new generation of sophisticated phishing attacks now target(ing) businesses. These phish evade traditional antivirus and anti-phishing products. Using targeted information - often gathered from social media sites - they fool even security-savvy employees into divulging sensitive information or visiting websites that infect machines with dangerous malware."
One very recent example of such a phishing expedition has been the recent deluge of emails directed against the faculty and staff of Lamar University, simultaneously directed at both their official ".edu" email addresses and their private email addresses. These multiple emails addressed to many of the employees are an apparent attempt to eventually bypass the security systems that are already in place; it does not really matter how good the university or corporate firewall or protective software, as many of the employees are also receiving redundant Phishing 2.0 emails at home, where the security may be likely to be weaker (or non-existent) than the professional security systems employed by the organizations. While the sophistication of the Phishing 2.0 attacks are intended to penetrate most common security methods, the simpler Phishing 1.0 still can wreak havoc on individuals and their employers.
Over the past few days, I have been made aware of multiple university employees, as well as employees of some of the other nearby colleges, receiving the following email at both their work and home email accounts; this email arrived numerous times over a two-day period at my home and work email addresses, as well as many of my acquaintances, both Lamar University faculty and staff and the faculty and staff of the other local lower division colleges:

From: Lamar Help Desk <helpdisk@lamar.edu>
To: Recipients <helpdisk@lamar.edu>
Sent: Thursday, November 21, 2013 2:20 AM
Subject: Mailbox Re-Validation

Your Lamar Password will expire in two (2) Days, click the link below to validate your e-mail
http://lamar(xxxxxxx).eu.pn/login.php

Thanks
Lamar Help Desk

Knowing that a percentage of recipients will always click on email links, it is inevitable that some users will be duped into doing that. At first glance, this email appears to be legitimate, unless the targeted victim looks closer at it. The item that attracted my primary attention is that I do not have a "lamar.edu" email address, as I teach at one of the other local colleges, but my wife, who does have a "lamar.edu" email address also received multiple copies of this Phishing email; I had also

received inquiries for other college faculty and staff who received this email.
While the simple header on this email appears to indicate that it is from the "Lamar Help Desk", notice that the word "helpdisk" is misspelled, with the suffix being "disk" rather than the correct "desk". The web link included in the email would also raise suspicion as to the real destination of the reply. While the beginning of the web address (URL) clearly says "lamar", there is a three word suffix (which I purposely redacted) creating a compound word after the prefix "lamar". Generally, the abbreviation ".eu" might indicate Europe, but this website actually has an upper level domain of ".pn" indicating that it is registered in the Pitcairn Islands. For those who may recognize the Pitcairn Islands in a historical context, these southern hemisphere, western Pacific islands are the home of the descendents of the mutineers of the famous British ship "The Bounty". I really do not see a Texas university having a major help desk located there. Examining the full headers of the phishing email, it appears to have originated on a server at the University of California - San Diego (UCSD), and been questioned by an IronPort spam filter, but still was delivered to many of its intended recipients. Many of these phishing emails also were not stopped by the generally very good spam filters utilized by several of the popular webmail providers, such as Gmail and Yahoo mail. It is possible that a hijacked account at UCSD was "milked" for information, providing the cyber crook with a list of attractive target ".edu" domains; it is also quite possible that the hijacked account at UCSD became a "zombie", unknowingly sending out spam emails at the request of a "Zombie Master" who may control thousands of compromised computers.
I also performed a basic digital trace of the link on the email, and found that the server that it is using is actually located in Kiel, Schleswig-Holstein, Germany. The registered owner of the server has a Russian sounding name, probably a pseudonym. Only generic information about the webhost was available, rather than the more common detailed contact information (also often bogus) of the actual website owner.
Using a "sandbox" on my computer (a virtual machine where nothing can get out and threaten my home computer), I tried to access the phishers' website, but was blocked by my memory resident security suite; even though I was likely safe, I decided not to continue to load the bogus website. Based on prior experience, the website would likely appear to be a legitimate Lamar University website where users would be asked to enter their username, old password, and new password. Since this is a bogus website, the new password would likely not be implemented, but either of two events will be likely to occur, both leading to the same nefarious results. The cyber crooks could either use the current username and password entered by the victim, or can change the password to one unknown to the legitimate user, preventing his access to any Lamar University system. This username and password is the necessary first step to logon to any computer at the university, allowing for email access as well as access to other data components at the university. Since the cyber crook now has an apparently legitimate Lamar University username and password, the email system now becomes available to the crook, as well as access to any accessible network drives. The amount of valuable data that can be stolen is immeasurable. The entire email history of the individual can now be downloaded, giving the crook information about students, family, and any other content, including passwords to external web services. It would be quick and easy for the crook to determine external web accounts that are connected to the now stolen Lamar.edu email accounts, go to those websites, click on the "forgot password" links, and have the external password or a reset link sent to the purloined email box. Not just would this process continue until the legitimate user contacts the real helpdesk and resets his password, but the identity theft will likely continue, until the legitimate user also changes any other external passwords linked to that compromised account.
This might just seem like a local issue, but Lamar, like most other universities, has faculty and staff engaged in research, such that the theft of the research (intellectual property theft) could result in financial loss, loss of a competitive advantage, and even a threat to national security, all because an employee clicked on an email link and thought that he was resetting an expiring password.
If anyone has ever clicked on this or the millions of similar emails asking for passwords, usernames, or credit card number confirmation, or responded to phone calls or text messages

informing the victim that his debit card number and PIN needs to be confirmed in order to reactivate the card, that person is likely to be the victim of identity theft.
While Phishing 2.0 is primarily intended to steal information from businesses and other organizations, the crude technology of the archaic, simple, but still effective Phishing 1.0 will still snare plenty of prey. In addition to the immediate changing of passwords (after scanning and removing any malware that may have been planted by the cyber crooks), it will likely be necessary to change other passwords, check credit bureau reports (totally free from annualcreditreport.com) and challenge any questionable postings. Complete information on dealing with identity theft can be found on the Federal Trade Commission website at www.consumer.ftc.gov/features/feature-0014-identity-theft.
Play it safe; be suspicious, adopt a policy of never clicking on links in emails, social networking sites, or instant messages (text messages). If, for example, you get an email apparently from your bank or a major retailer asking you to click on a link to verify information or sign up for something, do not perform that task by clicking on the link, but instead going directly to the known website of the source.
Be careful of what you click on; the results may be devastating.

Preserving memories in a digital age

Mike Hancock, Advertising Manager, Golden Gate Computer Society, CA
July 2013 issue, GGCS Newsletter www.ggcs.org editor (at) ggcs.org
More than 30 years ago—in 1982—videotapes came to the market. By now, though, many are degenerating. Alan Kolsky, of Digital Video Dimensions, startled attendees of the June 24 GGCS General Meeting by enumerating the probable life spans of various media:

- CDs 5 - 100 years
- Newspapers 10 - 20
- Data-grade VHS videotape 10 - 30
- Digital linear tape 10 - 300
- Other magnetic tape 10 - 30
- Microfilm 10 - 500
- Photographic slides 100
- Archival grade acid-free paper 10 - 500
- Egyptian stone tablet 2,000!

But people often want to digitize home movies, slides, videotapes, audio recordings, documents, and photos for storage and ease of presentation. Some authorities argue that because of rapid advances in technology enhanced media longevity is questionable.
Future trends that will affect archiving include higher resolution and solid-state storage. “4K” resolution video format (4,000 pixels in horizontal direction) is coming and is needed for the huge monitors, which tend to have much softer resolution than smaller monitors.
“Ultra HD” is on its way, too. 64GB thumb drives are readily available, and solid-state drives are being introduced to computers and will displace mechanical drives and players. DVDs are ubiquitous today, but Alan warned us that improper handling can rapidly degrade them. Hold DVDs at their edges, across their diameter; do not handle them on their recording face, and do not handle them roughly. Also, avoid using paper stick on labels because they cause wobbling and thus poorer recording.

These factors affect the life of any media:

- Quality of the original media. Kodachrome slides from the ’50s are still beautiful.
- The number of times the media are accessed.
- Storage temperature and humidity; store in a cool, dry place.
- Cleanliness of the storage environment.
- Quality of the device used to read/write the media.

To help keep your media in good condition:

- Keep media in its storage case.
- Avoid flexing or twisting any media.
- Do not touch exposed media.
- Do not expose magnetic media such as videotapes to magnetic fields (speakers, for example).

Alan recommends making backup copies of all digital media—two backups minimum for optical discs and hard drives. And re-copy them every two years or so. “High-8” tapes, especially from Sony, have a 20% failure rate, therefore they should be copied digitally and archived.

Tips for digitizing media

Alan suggests if you are digitizing home movie films to remember that film deteriorates and becomes brittle, and old projectors can accelerate damage.

With slides, look for at least 2,400-dpi scanners with no glass between the scanner and the film, otherwise you may have distortion from Newton rings, an interference pattern created by the reflection of light between two surfaces.

Canon is the best scanner brand for prosumers, or try to find an old Microtek 1800F on eBay. A 4,000dpi scan is the best, with 7,200 dpi being overkill, Alan says.

Document scanners are affordable at $500 to $600. Alan’s advice for scanning photos is to scan at 600 dpi for photos 5x7 inches or smaller, and at 300 dpi for greater than 5x7 inches.

Scanning services usually charge by the hour: $15 to $25. Be careful about cheap scanning services; they work as fast as possible and not necessarily with consistent quality. Also, pick out only the best of your photos to scan to reduce cost.

With videotape, “repack” the tape before copying by using fast-forward and fast-rewind before playback and capture. It helps, too, if tapes sit in the machine for a couple of hours before repacking because the heat of the machine makes them more flexible.

The best DVDs for general purposes are Verbatim and JVC at the Gold level. Ritek is another good general purpose DVD. Meritline.com and Rima.com are good online resources if you buy at least 50.

Go to eBay to obtain a Sony VHS Adaptor for the High-8 reader and capture the output of a VCR.

Alan showed us a couple of examples of advanced mixed media montages with voiceover, comprising slides, videos, and music. An external service would charge about $6,000 for a 35-minute professional mixed media show.

Video editing software include Adobe Premiere Pro, Sony Vega, ProShow Gold, and Photodex. Be careful, though, of copyright laws when using, for example, Youtube video clips or music. Alan recommends paying for royalty-free music or looking for government newsreels.

If you wish to digitize tape, look for a Grass Valley Digital Converter that runs output to a computer (upward of $250), or an outside service will do it for $25/hour. Clean dirty or greasy DVDs and CDs from the center out, radially, using a cleaner (Radio Shack has one).

Judging by the numerous questions and comments, a significant number of the audience had boxes of material that were candidates for digitizing!

Submit Your article; deadline for next bulletin is Tuesday noon each week. Only what you write may be published. We cannot publish other peoples work without written permission. Simply click here EDITOR AT TECC and paste your write-up to submit it.

Share your computer experiences with other members. We need articles to publish in the TECC Bulletin each week.

UPDATE YOUR MEMBERSHIP INFORMATION Change your e-mail address, unsubscribe to this bulletin, etc. Use link below.

UPDATE YOUR MEMBERSHIP