Managing Section Finances

GUARANTEED GET RICH QUICK!!
Managing Section Finances

Ken Pigg, SoutheastCon 4/1/2016
AGENDA

- Introduction
- Guidance
- Resources
- Advice
- Phishing Expedition
- Questions
Introduction

Ken Pigg
j.k.pigg@ieee.org
www.linkedin.com/in/kenpigg

- Region 3 Treasurer, MOVE Project Treasurer
- Past:
  - Region 5 Treasurer & Audit Committee
  - Section Treasurer – Oklahoma City and Eastern NC
  - NC Council Treasurer
- Long time Quicken user
Guidance

- IEEE Constitution & Bylaws
- IEEE Policies
- Financial Operations Manual
- IEEE chart of accounts
- MGA Operations Manual
- Region 3 Operations Manual
- Section bylaws, if they exist
  - Must be consistent with MGA Operations Manual
Resources

- IEEE Center for Leadership Excellence
  - Section Treasurer - Training
  - Section Treasurer - Job Description

- NetSuite training resources available within NetSuite and by request from finance-solutions@ieee.org
“Free” Advice

- Avoid any perception of impropriety
  - NEVER sign a check to yourself

- KSA – KEEP SHORT ACCOUNTS

- Utilize IEEE Concentration Banking (CB)

- NetSuite
  - Send request to finance-solutions@ieee.org for NEW credentials
  - Section Chair - ask for read only access

- Keep a copy

- Stay organized, ready for an audit
Phishing Expedition

- [email pdf]
- From and to are the “right people”
- NEVER be rushed
- NEVER send a wire without VERBALLY discussing it the requestor
- If you have any question, pick up the phone and call the requestor
Questions

Ken Pigg

j.k.pigg@ieee.org
Hi Ken,

I need you to make a payment of $1,710.00 today. Please get back to me immediately so I can send you the details for the payment.

Thanks,

Director,
Jim Conrad
Protect yourself

Cybercriminals may send you email that looks like it is coming from legitimate institutions, businesses and individuals you may know.

If you are unsure whether an email request is legitimate, consider contacting the institution, business or individual. Use information on an account statement or search for the company online but don’t use the contact information provided in the suspicious email.

Be careful of emails asking you to act immediately, especially if something sounds too good to be true. Think before taking any action.

Don’t click on attachments from unknown sources

Stop and Think before you Click!

Keep in mind that you could compromise your computer system and any personal or business information stored in it.

Not all websites are safe to use.

Potential Risks
- Identity theft
- Sensitive data loss
- Financial loss

To avoid potential risks, be cautious and take your time to review the website before taking any action.

Be Aware, Be Safe!

Avoid getting HOOKED!

IEEE IT Security

IEEE IT Security
Social Engineering Attacks

These attacks manipulate human interactions and our natural tendency to trust in order to gain access to confidential information (ex. usernames, passwords or bank information, etc.) for fraudulent or malicious activities.

Common Methods

**Phishing** - The attacker uses email, IM or other communication channels to impersonate a reputable person or organization to gain access to login credentials or account information.

**ViShing** - The attacker pretends to be a legitimate business and uses telephone conversations to attempt to scam the victim in order to gain access to information that will be used for identity theft.

**SMishing** - The attacker uses mobile text messages to lure the victim into calling back a fraudulent number, access a malicious website or download malicious content.

Use Strong Passwords

Use combinations of upper and lower case letters, numbers and Symbols

**Weak**: Webster

**Strong**: W3b$t3r

**Stronger**: A phras3 1s 3v3n Str0ng3r

How Phishing Works

**The Bait**
Email from the attacker encourages end user to follow a link to a spoofed web site that appears to be legitimate.

**The Hook**
A website controlled by the attacker that appears legitimate asking the victim to disclose information such as userid and password.
Beware and Protect Yourself Against Phishing Attempts Targeting IEEE Leadership Positions

The IEEE IT Security and Legal and Compliance departments have become aware of phishing attempts that try to leverage the credibility of IEEE leadership positions such as, but not limited to, Society Presidents, Region Treasures, Section Chairs, and Conference Organizers. These attempts are designed to manipulate the intended victim in order to gain access to money or private credentials.

Attackers may send you email that looks like it is coming from legitimate sources. These emails are often crafted quite well, and are getting increasingly difficult to spot. For example, the attacker may pose as an IEEE volunteer and ask you to transfer either funds or account information to the imposter. In these situations, the email address used by the attacker may even be designed to look like it is coming from a legitimate @ieee.org address or an address you may be familiar with.

Attackers research information about organizations (such as IEEE) to understand their leadership structure, gather names and contact information. This information is then used to spoof email address and create a message that looks realistic. Among the most common techniques attackers use to gain access to information are:

- The use of malicious links within email or websites that encourage intended victims to provide credentials or sensitive or financial information.
- Leveraging the use of malicious software (a.k.a. malware) to gather information from an infected system for fraudulent purposes. This software may be attached to email or may be available at a malicious or compromised website.
- Leveraging the use of automated password cracking tools to guess end user passwords (especially in cases where people are not using strong passwords).

To protect yourself against these fraudulent attempts the IEEE IT Security and Legal and Compliance Departments would like to offer the following tips and best practices:

- **Become familiar with and follow IEEE payment and financial processes.** If someone asks you to do something inconsistent with these processes over email, do not do it.

- **Be careful of wire transfer requests** – This is very common trick to gain access to money. In this case, a phisher might research organization websites or social media such as LinkedIn and find out the name of an IEEE leader. The phisher would then try to send an email that looks like it is coming from that leader requesting an immediate wire transfer. **One of the best ways to defeat this type of attack is to contact the person using a method other than the one you receive the request from. In other words, if you get an email, call them at a number that you know is legitimate. Do not use any contact information in the suspicious email.**

- **Always pay close attention to the actual address of the sender of the email.** It is quite common for a phisher to set up a fake domain with a similar looking name and then send mail from that account. For example, "bob@cern.org" and "bob@cem.org" can look the same at first glance.

- **Be careful with email that is not personally addressed to you,** or contains a generic name in the beginning of the email (e.g., Dear Sir). When you received these types of email the source should be questioned.

- **Be careful of emails asking you to act immediately.** If an email is portraying a sense of urgency where you have to act immediately or risk losing out, don’t do it. Some examples include wire or fund transfers or prizes you may have won that need credit card information to take care of miscellaneous fees.
• **Do not click on links or attachments received from unknown senders.** Keep in mind that you could compromise the security of your computer system and any personal or business information stored in it.

• **Be careful with password, password changes, or personal information requests.** In most cases, a legitimate business is familiar with phishing schemes and will not ask for you to supply a password, password change, or personal information via an email link. Don't supply the information (or click on the link for that matter). **If you think that the request is real, contact the person or business in another fashion** (such as a known Customer Service phone number). Use strong passwords, avoid sharing passwords, and keep passwords secure.

• **Pay attention to spelling mistakes and/or poor grammar.** It would seem that, with all of the work that phishers put into their trade, they would at least spell-check their document. Surprisingly, mistakes are still a telltale sign of a bogus email. In most cases businesses are pretty careful to send out pristine communications, so if there are spelling or grammatical errors, it may not be legitimate.

• **Be careful with “Friend or family member visiting <Country>”**. Many people have heard about the scam where an attacker tries to get you to provide them money. A twist on this scam has to do with a friend or relative in some kind of trouble, in a foreign country, that needs your money right now.

• **Verify email from questionable domains.** IEEE does business around the world, so there is always a chance that you could receive an email from anywhere. Take care in opening email from questionable or unfamiliar domains. There is a chance it is legitimate, but is worth verifying.

• **Be careful how much information you share on social media sites.** Do not share personally identifiable information or passwords through non-secure communication platforms. Avoid sharing information about your whereabouts such as vacation and travel plans. Attackers will use this information to make their phishing attempts more credible.

• **Trust your instincts.** If something does not feel right, take steps to confirm before acting. If you receive an email, call, or text requesting that you take an action, even if it is consistent with the responsibilities of your current IEEE leadership role, but you are unsure if it is legitimate please contact your supporting IEEE business unit and make them aware of the situation.

For additional information about targeted email scams: please refer to the following article published in IEEE Spectrum by Markus Jakobsson and William Leddy (Posted 21 Apr 2016):