



Section Finances

Ken Pigg, SoutheastCon 2018

AGENDA

- ▶ Introduction
- ▶ Guidance
- ▶ Resources
- ▶ Advice
- ▶ Budget
- ▶ Income
- ▶ Expenses

- ▶ Account Reconciliation
- ▶ Financial Status
- ▶ End of year Reporting
- ▶ Audit
- ▶ Phishing Trip
- ▶ Questions

Introduction

Ken Pigg

▶ Current Treasurer:

- Region 3
- MOVE Project
- Eastern North Carolina Section
- SoutheastCon 2020

▶ Past:

- Region 5 Treasurer & Audit Committee
- Section Treasurer – Oklahoma City and Eastern NC
- NC Council Treasurer

Survey Says . . .

Section volunteer role

Section Chairs?

Section Treasurers?

Financial wizardry level?

Have never reconciled a checking account?

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 by request from finance-solutions@ieee.org
 - Task specific instructions available inside NetSuite

“Free” Advice

- ▶ **Avoid any perception of impropriety**
- ▶ 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

Budget

- ▶ Start by December for the upcoming year
- ▶ It is a plan – it can be revised
- ▶ Typically approved by Section Committee
- ▶ Use IEEE MGA chart of accounts
- ▶ Chapters must be funded
- ▶ Sub categories
 - Take out the middle man

Income

- ▶ Annual rebate, based on:
 - Meetings reported (section and chapters)
 - Number of members
 - Number of chapters
 - Timely Reporting Bonus – 10%
- ▶ Conference sponsorship – with risk
- ▶ Other local events
- ▶ Mail in deposits (for CB accounts)

Expenses

- ▶ [Region 3 travel policy](#)
- ▶ [Region 3 expense report form](#)
- ▶ Concentration Banking (CB) debit card
- ▶ Get receipts and document purpose
- ▶ Section Chair typically should be a checking account signer
- ▶ MGA “tax” (“7 Reserve Allocation Expense”) being eliminated!

Reserves

- ▶ <http://www.ieee.org/documents/section03109903.pdf>
- ▶ 3.2 ADMINISTRATION OF MGA FINANCES
 - A. Reserves.
 - Per the IEEE Financial Operations Manual, the MGA Board will try to maintain reserves of about **50% of annual expenses**, exclusive of those dedicated to Sections Congress.
- ▶ Region 3 Operations manual, Section III says 35% to 50% of average expenses over last 4 years

Account Reconciliation

- ▶ Do it monthly, as soon as bank statements are available
- ▶ Run reconciliation report

Financial Status

- ▶ Publish reports monthly, as soon as reconciliation completed
- ▶ Reports
 - Income Statement
 - Budget Report
 - Balance Sheet
 - Reconciliation Report
- ▶ Treasurers report should be on each EXCOM agenda

End of Year Reporting

- ▶ Same reports as monthly but for the full year
- ▶ Section includes chapters and affinity groups but not student branches
- ▶ No more L50, all transaction in NetSuite
- ▶ Notify finance-solutions@ieee.org that NetSuite is ready for review
- ▶ 10% early reporting bonus deadline 3rd Friday of February
- ▶ Drop dead for section rebate end of February

Compliance Reporting

- Conflict of Interest, banking signature cards, etc.
- [IEEE Financial Reporting web page](#)

Audit

- ▶ Prior year, after reporting complete
- ▶ Required if revenue or expenses > \$250k
- ▶ Self audit guide and checklist available
- ▶ Treasurer wants some form of audit as a CYA

Phishing Expedition

- ▶ 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



Spear Phishing

Ken Pigg

From: Jim Conrad <jmconrad@uncc.edu>
Sent: Friday, March 17, 2017 10:44 AM
To: j.k.pigg@ieee.org
Subject: Wire Transfer

Ken,

Are you at your desk? I'll need you to process a Wire Transfer to a vendor. Let me know when you will be available for the instructions.

Regards,
Jim

Spear Phishing

Ken Pigg

From: Director Jim Conrad <jmconrad@uncc.edu>
Sent: Thursday, March 9, 2017 1:51 PM
To: j.k.pigg@ieee.org
Subject: FUNDS NEEDED

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

Spear Phishing

From: Matthias Horrer <cchairmann@aol.com>
Sent: Monday, February 26, 2018 12:28 PM
To: ieee@pigg.us
Subject: EXPENSE REIMBURSEMENT

Hello,

How are you doing? Would like you to carry out a transaction, get back to me as soon as you get this so that i can instruct you on how to proceed with it.

Enjoy the rest of the day.
Matthias Horrer

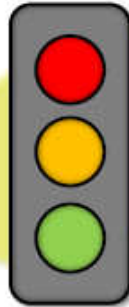
IEEE Flyer

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.



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!



Cybersecurity Awareness

Protect Yourself



Avoid getting HOOKED!

IEEE IT Security



IEEE Flyer

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.

! WARNING

- Don't click on links or attachments received from unknown senders
- When verifying the sender, do not use the information in the suspicious email
- Be careful of how much information you share on social media sites
- Don't assume a caller is genuine because they know about you or your company - If suspicious, terminate the call

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.

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



Consider making your password a phrase: A phrase can be used to create a strong password. Consider using at least 12 characters. Use phrases that are easy to remember but hard for someone else to guess.

Use unique accounts & passwords: Using different passwords for every account helps to thwart attackers. At a minimum, separate your work and personal accounts. Make sure that your critical accounts have the strongest passwords.

If you write it down then keep it safe: Store your list in a safe, secure place away from your computer. You can consider using a password manager application to keep it safe and track your passwords.

Spectrum Article

- ▶ **Beware and Protect Yourself Against Phishing Attempts Targeting IEEE Leadership Positions**

- <http://spectrum.ieee.org/telecom/security/fighting-todays-targeted-email-scams>

Questions?

Ken Pigg

j.k.pigg@ieee.org

www.linkedin.com/in/kenpigg