DAC db UNIVERSITY

District and Club database

Information Security and You

Overview

- Introduction / Overview
- Email scams
- Things you should do
- Club/District Information Sharing
- Club/District Websites
- What DACdb stores and does not store
- Bottom line

A few facts

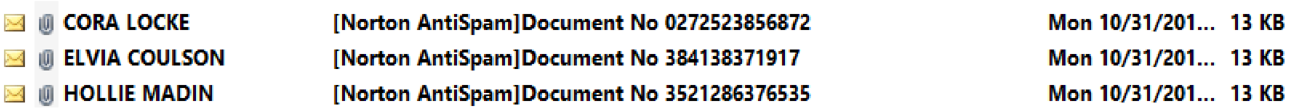
- Many users have *Little* to *No* concept of security
- Users use *terrible* passwords
  - E.g. "*A*" or "*password*" or their *First Name* or *{firstname}123*
- Many clubs and/or districts publish their content on public websites
- WIFI Locations can be easily tapped
- Websites are scanned daily by ***bots*** that look at ALL publicly available content

Email

- Email is insecure
  - Nearly all emails are sent in plain-text
- Email names and addresses can be spoofed
  - Anyone can send you an email that looks like it's from anyone else
- Email content can contain viruses/malware
  - Don't open emails from users you do not know or trust
  - Turn off preview viewers – which do "open" emails
- Email attachments likely contain viruses/malware
  - Never open ZIP and EXE files from someone you do not know

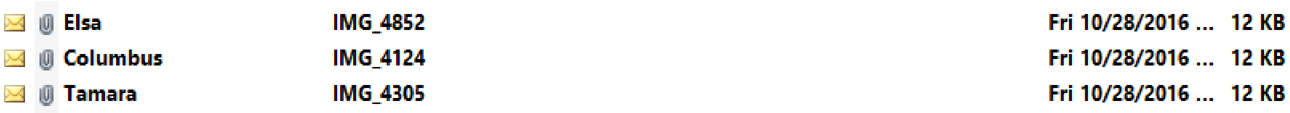
Phishing Email Examples

- Phishing emails are “fishing” for your information
  - Zip Files



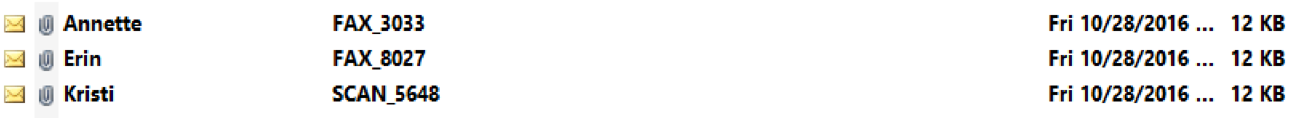
✉	📎	CORA LOCKE	[Norton AntiSpam]Document No 0272523856872	Mon 10/31/201...	13 KB
✉	📎	ELVIA COULSON	[Norton AntiSpam]Document No 384138371917	Mon 10/31/201...	13 KB
✉	📎	HOLLIE MADIN	[Norton AntiSpam]Document No 3521286376535	Mon 10/31/201...	13 KB

  - Image files



✉	📎	Elsa	IMG_4852	Fri 10/28/2016 ...	12 KB
✉	📎	Columbus	IMG_4124	Fri 10/28/2016 ...	12 KB
✉	📎	Tamara	IMG_4305	Fri 10/28/2016 ...	12 KB

  - Faxes and Scans



✉	📎	Annette	FAX_3033	Fri 10/28/2016 ...	12 KB
✉	📎	Erin	FAX_8027	Fri 10/28/2016 ...	12 KB
✉	📎	Kristi	SCAN_5648	Fri 10/28/2016 ...	12 KB

Email Scam Examples

- Example 1

Tips:
Do it today!

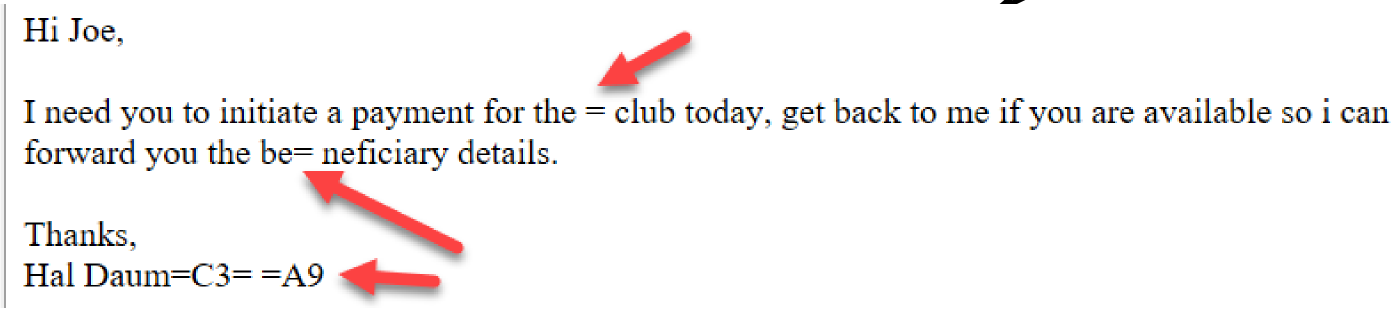
Hi (treasurer first name)

Hope all is well. I would like you to process a payment to a vendor. Kindly email to let me know if it can be done today so I can email you the payment instructions now.

Thanks,
(President's first name)

- Example 2

Tips:
punctuation



Hi Joe,

I need you to initiate a payment for the = club today, get back to me if you are available so i can forward you the be= neficiary details.

Thanks,
Hal Daum=C3= =A9

Email Scam Examples

- A more complicated thread:

Tips:
mal-formed HTML
grammar

From: {name email redacted}
To: {email redacted}
Subject: Re: Attn – (name redacted)
Date: Tue, 22 Nov 2016 09:42:16 -0700

{Redacted} Sorry {Redacted},I'm having a mouth ulcers
,can't speak up on phone!Can you please confirm to me our
available balance as soon as possible in other to send out
to you details and information to proceed with the
transfer.Waiting to read from you!Thanks,{name redacted}Call
me 519-817-8589----- Original Message Follows
-----From: {name email redacted} To:
{email redacted}Subject: Attn – {name redacted}Date: Tue,
22 Nov 2016 04:47:12 -0700>{redacted},I need you to set up
a bank transfer for a>payment ,let me know if you can
handle this right away so I>can send you the bank details
and can you please confirm to>me the available current
account balance .waiting for>your reply.Thanks.{name
redacted}.
</blockquote></BODY>

Email Scam Examples

- Another example:

Hi {name redacted}

I will need your help to make a transfer into the a
account details as follows:

Bank Name:CHASE Bank
Account Name: {Name Redacted}
Account Number:738789283
Routing Number :322271627
Bank Address:17317 Main St,Hesperia,CA 92345

Amount to be transfer:$71,150.00

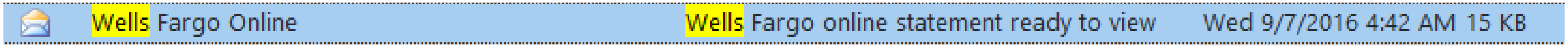
Let me know when the transfer is done .I will be waiting for your email with the payment confirmation copy.I will really appreciate if you could get this done for me swiftly .

Waiting to read from you

Tips:
Verify owner with Bank
Out of town Bank
Pressure to act fast
Syntax: double periods, no space

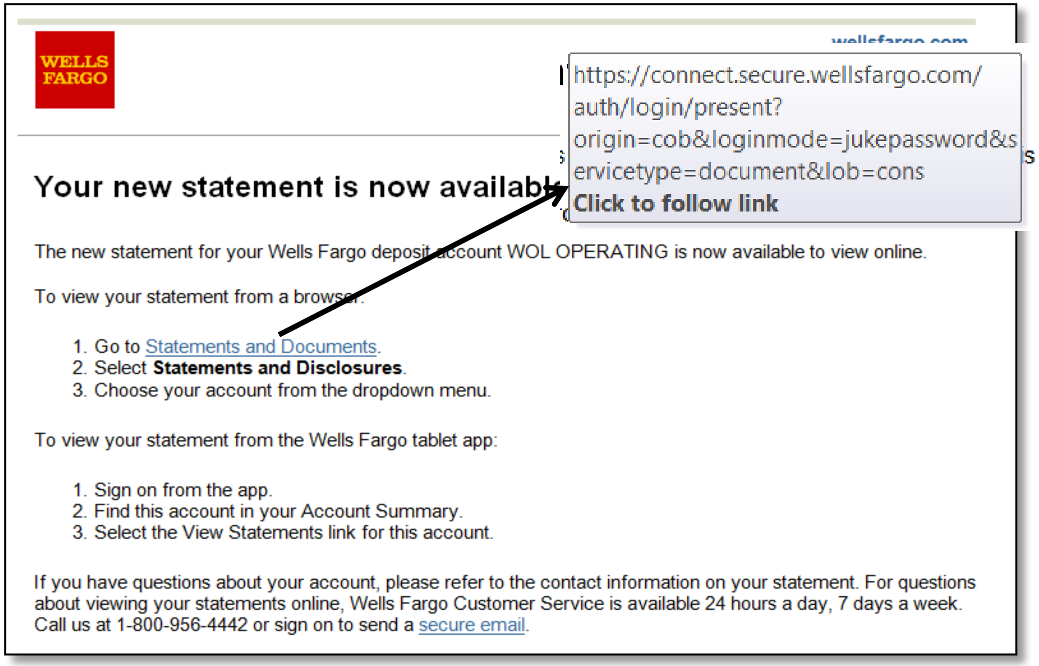
Emails: from your bank

- Ignore emails from your Bank



Wells Fargo Online Wells Fargo online statement ready to view Wed 9/7/2016 4:42 AM 15 KB

  - Easy to duplicate
  - Sent by anyone
  - Links off to shell Sites to capture credentials



https://connect.secure.wellsfargo.com/auth/login/present?origin=cob&loginmode=jukepassword&servicetype=document&lob=cons

Your new statement is now availabl

The new statement for your Wells Fargo deposit account WOL OPERATING is now available to view online.

To view your statement from a browser:

1. Go to Statements and Documents.
2. Select **Statements and Disclosures**.
3. Choose your account from the dropdown menu.

To view your statement from the Wells Fargo tablet app:

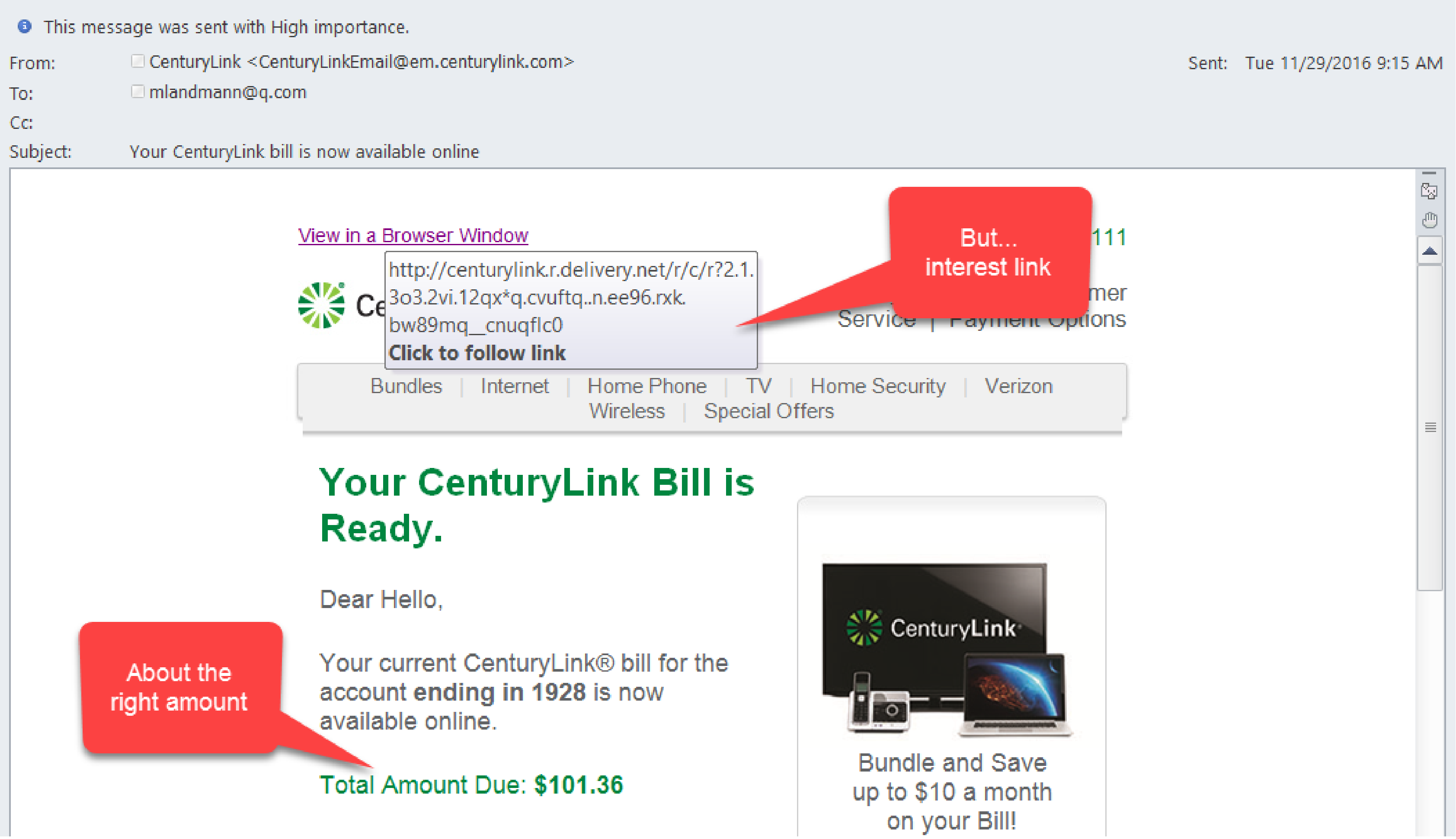
1. Sign on from the app.
2. Find this account in your Account Summary.
3. Select the View Statements link for this account.

If you have questions about your account, please refer to the contact information on your statement. For questions about viewing your statements online, Wells Fargo Customer Service is available 24 hours a day, 7 days a week. Call us at 1-800-956-4442 or sign on to send a secure email.

- Go online directly yourself – not via an email link
- If you have to – look at the link – CAREFULLY!!!

Emails: from your telco

- Ignore emails from your phone company



This message was sent with High importance.

From: CenturyLink <CenturyLinkEmail@em.centurylink.com>

Sent: Tue 11/29/2016 9:15 AM

To: mlandmann@q.com

Cc:

Subject: Your CenturyLink bill is now available online

View in a Browser Window

http://centurylink.r.delivery.net/r/c/r?2.1.3o3.2vi.12qx*q.cvuftq..n.ee96.rxk.bw89mq__cnuqflc0
Click to follow link

But... interest link

Service | Payment Options

Bundles | Internet | Home Phone | TV | Home Security | Verizon Wireless | Special Offers

Your CenturyLink Bill is Ready.

Dear Hello,

Your current CenturyLink® bill for the account **ending in 1928** is now available online.

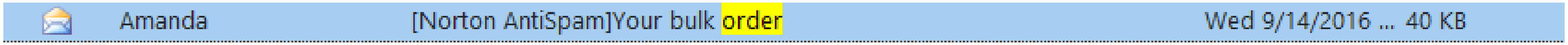
About the right amount

Total Amount Due: **$101.36**

Bundle and Save up to $10 a month on your Bill!

Emails: order confirmations

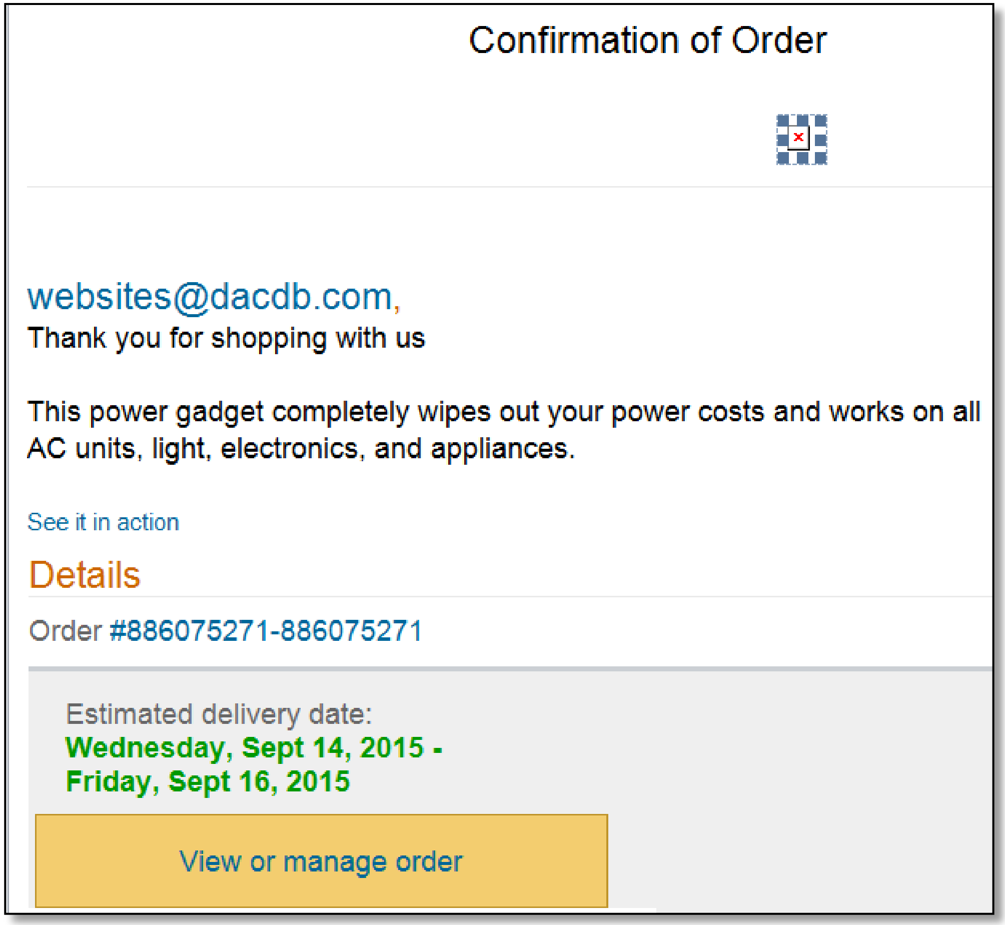
- Unsolicited order confirmations



Amanda [Norton AntiSpam]Your bulk order Wed 9/14/2016 ... 40 KB

- Don't click on the links

- Go directly to vendor's site
  - or –
  FedEx/UPS tracking



Confirmation of Order

websites@dacdb.com,
Thank you for shopping with us

This power gadget completely wipes out your power costs and works on all AC units, light, electronics, and appliances.

See it in action

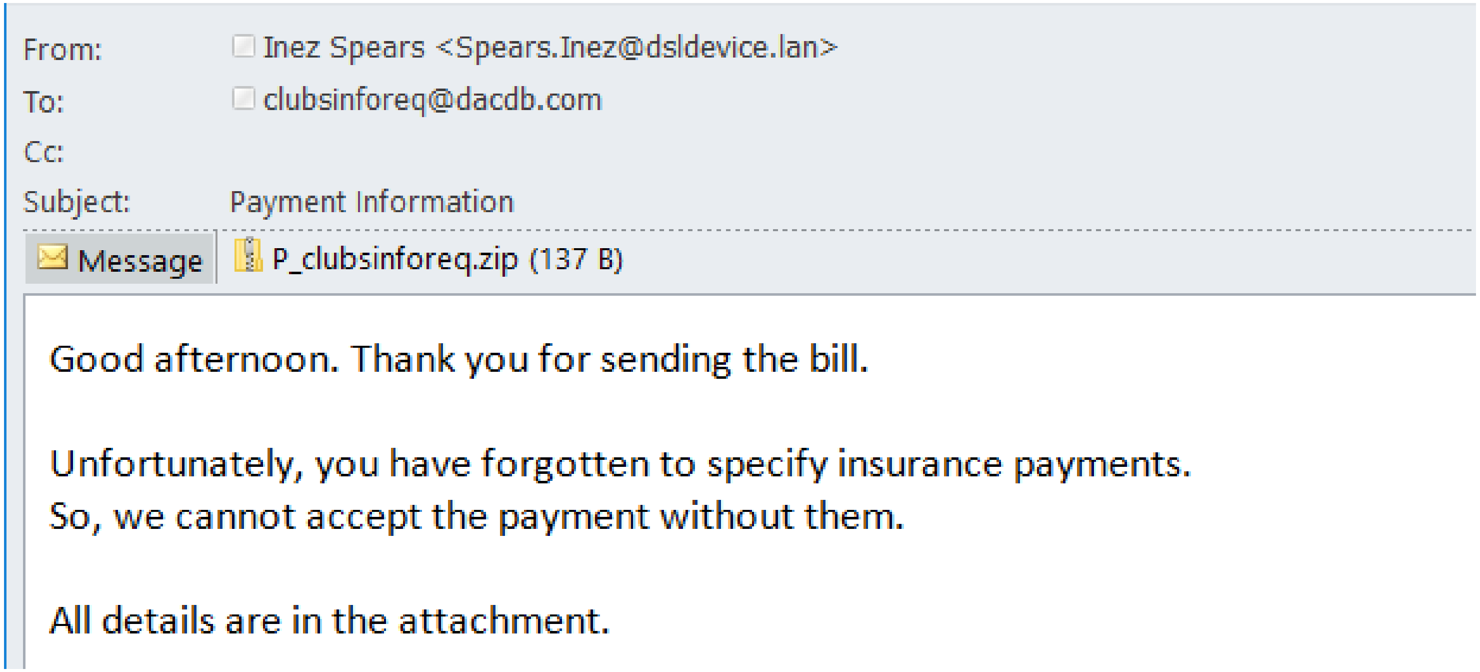
Details

Order #886075271-886075271

Estimated delivery date:
Wednesday, Sept 14, 2015 -
Friday, Sept 16, 2015

Emails: Zipped Invoices

- DO NOT click on ZIP files!!
- Ignore requests for more information / payments



From: □ Inez Spears <Spears.Inez@dsldevice.lan>

To: □ clubsinforeq@dacdb.com

Cc:

Subject: Payment Information

P_clubsinforeq.zip (137 B)

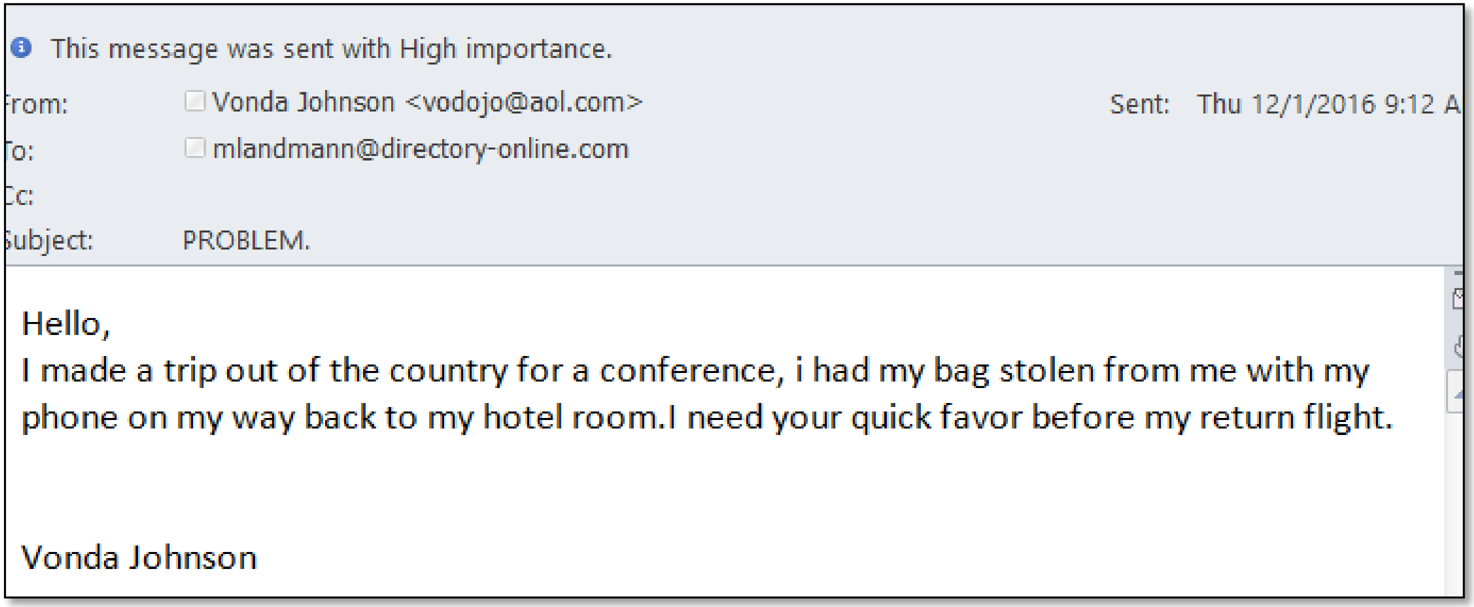
Good afternoon. Thank you for sending the bill.

Unfortunately, you have forgotten to specify insurance payments.
So, we cannot accept the payment without them.

All details are in the attachment.

Emails: Help – out of the country

- Need money to get home – no you don’t!!



This message was sent with High importance.

rom: □ Vonda Johnson <vodojo@aol.com> Sent: Thu 12/1/2016 9:12 A

o: □ mlandmann@directory-online.com

c:

ubject: PROBLEM.

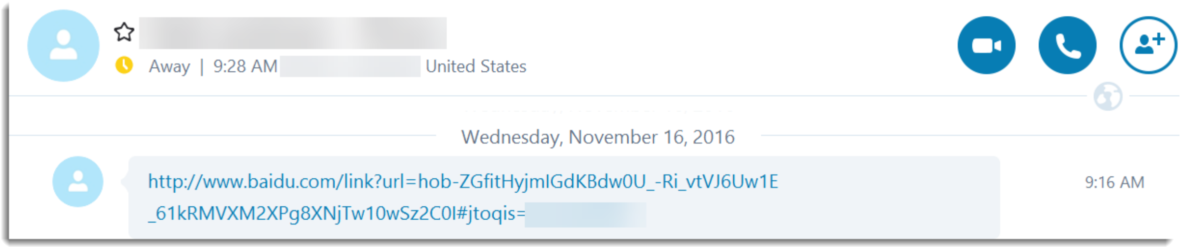
Hello,
I made a trip out of the country for a conference, i had my bag stolen from me with my phone on my way back to my hotel room.I need your quick favor before my return flight.

Vonda Johnson

- A Prince wants to share a huge some with you?
  - Nope – your not going to get rich playing along

Skype: links & friend requests

- Please DO NOT:
  - Click on strange looking links (even from friends)



[redacted]

Away | 9:28 AM [redacted] United States

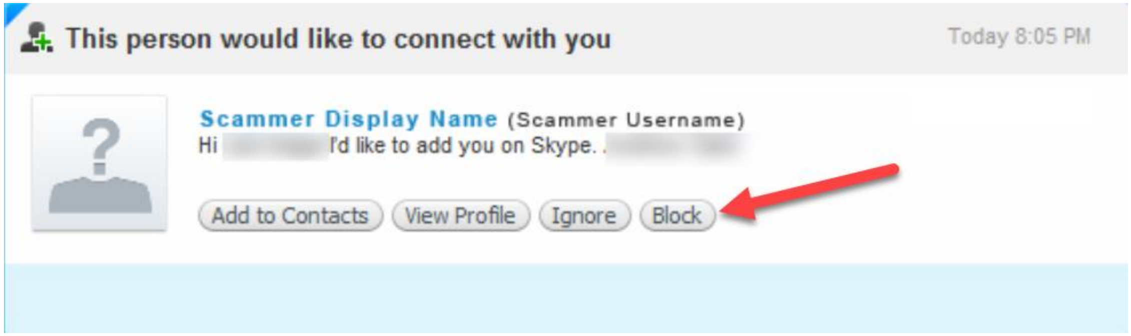
Wednesday, November 16, 2016

http://www.baidu.com/link?url=hob-ZGfitHyjmIGdKBdw0U_-Ri_vtVJ6Uw1E_61kRMVXM2XPg8XNjTw10wSz2C0I#jtoqis=[redacted]

9:16 AM

  - Accept friend requests from people you DON'T know

- Best Practice:
  - *Block* unsolicited friend requests and spammers



This person would like to connect with you

Today 8:05 PM

Scammer Display Name (Scammer Username)

Hi [redacted] I'd like to add you on Skype. [redacted]

Things you should do

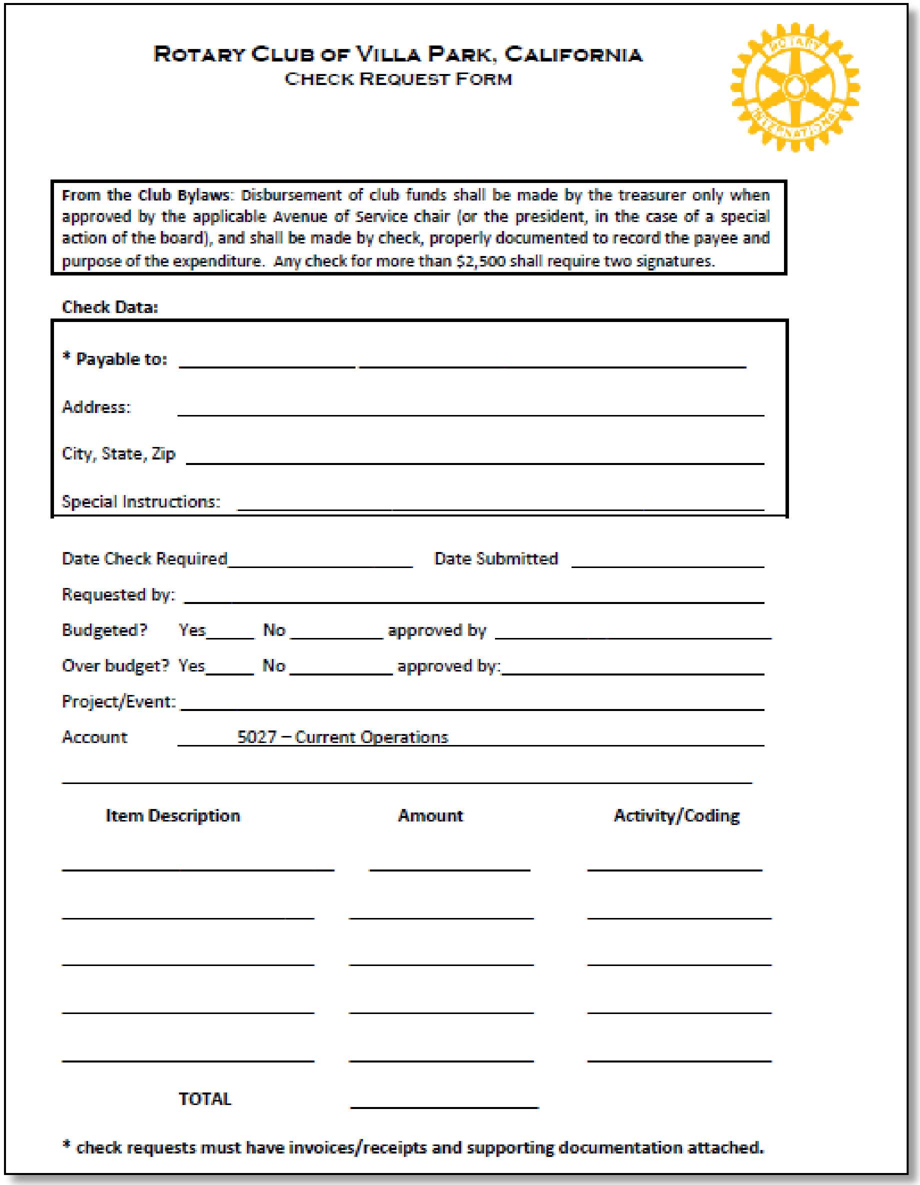
- Members
  - Change your password:
    - Change MemberID or ZipCode password to something else
  - Use STRONG Passwords!!:
    - 8 characters or more
    - Upper/lower case
    - Numbers
    - Special Characters ($^&*!)
  - Use different passwords on different websites
  - Think about your security levels – who needs access to what

Things you should do

- Clubs/Districts
  - Information Sharing
    - Evaluate EVERYTHING posted on the websites and/or club bulletins and district newsletters
  - Implement a Club/District Communications Officer that has responsibility for information sharing
  - Make sure your webmaster is well-versed in security and data protection
  - Use STRONG passwords for website administration
  - Procedures:
    - Implement a standard CHECK REQUEST form
    - Pay no invoice without an invoice counter signed by the project chairman or responsible party
    - Counter-sign invoices for payment
    - Implement dual-signature checks

Example Check Request Form

- Check Request Form example
  - With thanks to RC of Villa Park



ROTARY CLUB OF VILLA PARK, CALIFORNIA
CHECK REQUEST FORM

From the Club Bylaws: Disbursement of club funds shall be made by the treasurer only when approved by the applicable Avenue of Service chair (or the president, in the case of a special action of the board), and shall be made by check, properly documented to record the payee and purpose of the expenditure. Any check for more than $2,500 shall require two signatures.

Check Data:

*** Payable to:** ______________________________

Address: ______________________________

City, State, Zip ______________________________

Special Instructions: ______________________________

Date Check Required__________________ Date Submitted __________________

Requested by: ______________________________

Budgeted? Yes_____ No _________ approved by ____________________

Over budget? Yes_____ No __________ approved by:____________________

Project/Event: ______________________________

Account 5027 – Current Operations

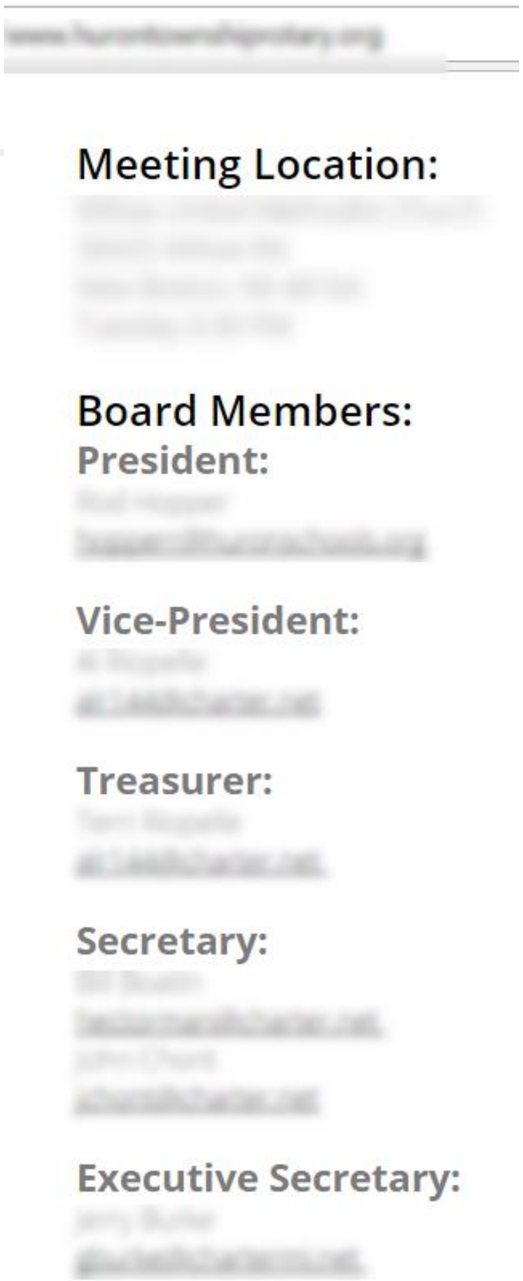
Item Description	Amount	Activity/Coding
TOTAL		

* check requests must have invoices/receipts and supporting documentation attached.

Websites

- Please DO NOT:
  - Include email addresses on websites
  - Include phone numbers of members
  - Use weak admin passwords

- Best Practice:
  - Use built-in DACdb blindside email links
  - Limit information about members
  - Limit publication of documents with personal data
- Notes:
  - Evaluate the risks of where and when emails are exposed (e.g., maybe district leaders on a district site)



[redacted]

Meeting Location:

[redacted]

Board Members:

President:

[redacted]

Vice-President:

[redacted]

Treasurer:

[redacted]

Secretary:

[redacted]

Executive Secretary:

[redacted]

Websites

- Please DO NOT:
  - Include links to a complete District Directory
  - Include district and club financials
    - (It may need to be public – but not for the World)

- Best Practice:
  - Use “Secure Files”

What does DACdb store?

- Member Information (Info Tab)
- Spouse / Partner Information (Spouse Tab)
- Contact Information (Contact Tab)
  - Email
  - Address
  - Social Media Links
  - Phone Numbers
- Participation Data (PData Tab)
- RLI Class Information (Class Tab) (new)
- Bio/Degree information (Bio/Notes)
- Club Officer Positions (Club Edit)

DACdb does **NOT** Store

- Credit Card numbers
  - Including expiration dates and CVV (number on back)
- TRF Contributions
  - We print out a form which is not saved
- Social Security Numbers
- Other sensitive data
  - DACdb stores almost nothing that can't be found with some persistent Googling.

Responsibilities

- Clubs and Districts are responsible for:
  - ALL content they post – especially on public websites and published materials
  - Assigning appropriate security levels to members
  - Ensuring that club/district officers, and other members, are aware of, and follow, both RI and club/district rules and procedures

- DACdb is responsible for:
  - Securing user credentials
  - Securing Secure Files system
  - Keeping the database secure

The Bottom Line

- The internet is not safe. PERIOD!!
- There are 100,000's out there trying to hack/scam you
  - Kids in China are not fed until they hack you!!
- So easy to steal an identity – so difficult to fix it.
- This season: over 1,100 fictitious websites
- There are tons of phishing emails!!
  - Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels.
- DO NOT rush or feel pressured
- If you go to foreign countries, assume ALL your connections are being monitored, tracked and captured!
  - (and yes, assume the NSA is doing same here)

The Bottom Line

- You need to be on the defensive:
  - Think before you click that link – do you know who sent it?
  - Think before you act – one wrong click and you're "hit"
  - Open emails only from people you know – the others are NOT your friends
  - Never INSERT a thumb drive you find laying around
- Use STRONG passwords
- Protect your assets – bank, stocks, etc.
  - Don't shop (pay) online using public WIFI
  - Use different STRONG passwords on EVERY website
- Do not access strategic assets on public WIFI
  - Simply wait until you get home or call the bank/broker
- Do not divulge financials via Email – Pick up a phone!

Take a Test

- Google and/or Bing:
  - Rotary District XXXX club officers
  - Rotary Club of XXXX club officers
  - Rotary Club of XXXX club members
  - {a member name} or Your Name
- Social Media
  - Review Facebook, Twitter, LinkedIn and other sites
- Ask yourself the question:
  - Am I (are we) sharing too much information?
  - Do we want the hackers, Russians, Chinese or North Koreans to see this information?

Reference Material

- Here is some more information about email spoofing:
  - https://en.wikipedia.org/wiki/Email_spoofing
- Here is a site to reverse engineer IP addresses:
  - www.IP2Location.com
- phishing
  - http://searchsecurity.techtarget.com/definition/phishing