VISTA ROYALE COMPUTER CLUB

February 3, 2022

Mike Johnson welcomed everyone and announced that we have about 57 members so far this season and are still accepting your $20 cash dues for 2022. He then introduced Vicky Getz and her very timely presentation. Here are her notes. We will announce our Feb 10th presenter in the reminder the first of next week. Regards, Sandy McKenny, Sec

Vicky Getz talked about the SPOOFING AND SPAM,

She had originally planned on presenting about how to evaluate links and phishing attempts, but on Sunday when looking for good examples for phishing she found a current campaign where a spammer was pretending to be people she knew from Vista Royale,

=====
SPAM
=====

Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk.

Initially a legitimate marketing tool, bulk email quickly developed into a tool for selling shady products, and then into a tool for stealing from you.

Malicious spam is increasingly used by large well financed criminal organizations and state sponsored organizations to steal your personal data, which they then sell on the dark web, ransom your data, or turn your computer into a zombie to launch a denial-of-service attacks against companies.

==========
SPAM FILTER
==========

Most email services have built-in tools for detecting junk mail and moving them to another location (usually a folder called “Spam” or “Junk”) where you can still see them or ignore them forever.

Over the course of the pandemic - particularly in the past six months - many people have noticed a surge of malicious emails slipping through the spam filters and landing in their inboxes.

Spam is getting harder and harder to detect.

These criminals are using social engineering techniques to:

Get you to open a malicious attachment
Send you to a lookalike site to trick you into entering information.
Send you to websites that do drive-by-download of malware.

One of the big tools they use to fool you is spoofing

Since most of us understand that links and attachments from strangers are dangerous, spammers try to get us to believe they are a company we do business with your friend, spammers often change the display name to gain our trust. This is called spoofing.

==========
SPOOFING EXAMPLE
==========

When you get an email from us it will say:

From: Vista Royale Computer Club

If it was truly from us then the email address would be

From: Vista Royale Computer Club <vrcomputerclub @ gmail.com>

A spoofed address would still display Vista Royale Computer Club but would come from a different email address.

From: Vista Royale Computer Club <spamersaccout @ hotmail.com>

==========
SPOOFING COMPANIES
==========

We looked at a spam mail spoofing Amazon

Your Account is locked
no-reply @ amazon.com

==========
SPOOFING YOUR FRIENDS
==========

In order to pretend to be someone you know, they don't need access to your email account nor your friends, although they may have it. No, all they need is a list of related contacts that contains the following information.

First Name, Last Name, email address

Spammers are very creative in getting these lists of related contacts.

Infecting a user's computer with malware

Contact harvesting apps planted in the official app stores.

Breaches of email sites

Breaches of social media sites ….

Finding an online member directory...

Getting their hands on those much-forwarded email jokes, where the forwarders never cleared the headers that contain a list of all the recipients.

==========
Current Vista Royale Spoofing
==========

In looking for examples of evil spam, Vicky found a spoofing campaign where a spammer is impersonating several people she knows at Vista Royale. The Vista Royale Computer Club is on the list, as are Vicky and Sandy are among the small sampling she saw. If you receive odd looking emails from us that have nothing to do with the computer club, we urge you to inspect the sender address.

==========
CURIOSITY KILLED THE CAT
==========

Curiosity Killed the Cat

Be suspicious of links and attachments even if they appear to be a company you deal with, or a person you know.

Ask yourself, does the email look right?

Verify the Contact by looking beyond the **Display Nam**e at the raw email address?

If you are not sure if the raw email address is supposed to be

If you have contacted them before, you can start composing an email to them and when you enter the TO field their raw email address appears.

Of course, if the email seems out of character, it could be that your contact really has been hacked. Contact the sender by an alternate method.to see if they sent the message.

==========
SPAM or JUNK EMAILS
==========

Some “experts” recommend setting up an email filter rule to send all emails from people not in your contact list to your spam folder. In practice this causes people to have to routinely search their spam folder for incoming emails.

Your email provider's spam filter puts these emails in your Spam/Junk folder because it thought they were dangerous.

SPAM = JUNK = Danger!

Avoid rummaging through your spam/junk folder.

Only check the spam/Junk folder if an expected email is missing.

Some emails go in spam by mistake, but the evil emails that are in there can look like something you should open.

Trash is not the same as Junk, your trash folder contains your files you deleted.

==========
DO NOT UNSUBSCRIBE
==========

Legitimate companies are not going to direct-market to you without a prior relationship with you. Legitimate companies always ask you if you want to sign up for their mailing list, often by a sneaky little box that you need to uncheck when you create an account with them.

If you receive unsolicited bulk email, **do NOT** use the unsubscribe link provide and **do NOT reply**, simply mark it as spam or junk or delete it.

If you are **SURE** that you signed up for the mailing list or have created an account with them without unchecking the box allowing them to contact you with special offers, only then can you safely use the unsubscribe link provided.

==========
Good Practices
==========

Never open attachments from strangers!

Never follow links from strangers!

Only open attachments that you are EXPECTING

Don't follow links if the email is out of character for the sender.

Verify the sender, is the sender

Past meeting minutes can be viewed at our website http://www.vrcc.info/