



LOCAL GOVERNMENT CYBERSECURITY

BUD RITCHIE
CITY OF HARRISONBURG

Disclaimer



Agenda

- Cyber Overview
- Phishing Attacks
- Passphrases
- Local attacks
- Q/A

What Threats?

- Social Engineering
 - Phishing
 - Smishing
 - Vishing
- Credential Attacks
 - Theft
 - Default Passwords



```
position: absolute; z-index: 999  
x 5px #ccc}.gbrtl .gbm/  
display: block; position  
opacity: 1; *top: -2px; *le  
/; top: -4px\0/; left: -6  
ne-box; display: inline  
display: block; list-s  
e-block; line-height  
pointer; display: bl  
tive; z-index: 1000)  
padding-right: 9px  
durl111
```

Phishing

Tips to Identify a Phishing Email

- Sense of Urgency
- Unfamiliar sender
- Requests for PII or other data
- Generic greetings
- Email Address/name mismatch
- Spelling/grammar

Sample Phishing Emails

From: [REDACTED] <v14ida@gmail.com> **Unknown**
Sent: Monday, July 11, 2022 12:28 PM **Sender/Username**
To: [REDACTED]
Subject: DD: Change

WARNING: This email was sent from outside of your organization.

Hi, [REDACTED] **Unnecessary punctuation**

I recently changed my financial institution and want to update my account information in the system for the next payroll run. Can I email you the bank information and a voided check to have the details updated? Also let me know the payroll date the change would be effective for after making changes. Let me know how to proceed.

Thank you,
[REDACTED]
[REDACTED]

From: Martin joseph <andersondickson210@gmail.com>

Sent: Saturday, August 6, 2022 5:09 AM

Subject: [BULK] Condolences Notice!

Importance: Low

WARNING: This email was sent from outside of your organization.

--
Condolences Notice!

We welcomed Mr. Mike and Mrs. Elizabeth yesterday evening at our office with a painful report that you had an accident three days ago and couldn't survive the accident when you was on your way to work.

They claimed that they are your siblings that they seriously need your fund to prepare your burial ceremony which they came with \$100 to clear all the necessary charge and claim your fund.

If you're not dead,please kindly respond now and have your fund before it's too late but If you're truly dead,may your soul rest in peace.

We should release your fund to them to conduct your burial smoothly as they requested if we didn't hear from you in the next two days.

May your spirit avenge who ever caused your sudden death.Amen

Best regard

Mr. ROBERT REDMAN

Tricky sample



VA DMV <dmv@compliance-gov.com> (VA DMV via ispservices.org)

To ✓ Bud Ritchie

i If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.

Start your reply all with:

Completed.

This has been completed.

Will do, thank you.

i Feedback

WARNING: External email. Be cautious when clicking on links or opening attachments.

Hi Bud,

Due to an update to our new compliance system, all users must update their contact information.

Update now at: <https://www.compliance-gov.com/dmv-update>

Please complete this update by April 29, 2024 to avoid any penalties.

Thank you,
VA DMV

VA DMV

<https://secured-login.net/xdxjqspwh0dhkbzoi8vc2gvjdxjlxzc1scb2dpbi5umzxyqvcgfnzmvntjlmte2gyjq2mzqznizlbwfpbf90zw1wbgf0zv9pzd0ymde5njjwjmfdglvbj1wcmv2awv3jnvzzxfawq9njlxmtuwntq=>
Click or tap to follow link.

From: Mark Reed <mark1219@mailbox-gmail.com>

Sent: Tuesday, June 6, 2023 3:02 PM

To: Rebecca Huffman <Rebecca.Huffman@harrisonburgva.gov>

Subject: food poisoning

WARNING: This email was sent from outside of your organization.

Dear Sirs,

My family visited your location last week and my wife had a complicated case of extreme food poisoning after the visit. We initially thought that she had an allergic reaction, but it appears her reaction was caused by the quality of the food you served us. My attorney is preparing a lawsuit, and in the attached form you can see the initial doctor's opinion disclosed. I would prefer to settle this issue unofficially for the convenience of both parties involved.

Thank you.

Regards,
Mark Reed

From: Graham Nelson <graham@matchboxrealty.com>
Sent: Wednesday, August 24, 2022 2:29 PM
To: Pamela S. Ulmer <Pamela.Ulmer@harrisonburgva.gov>
Subject: Re: email - dropbox

WARNING: This email was sent from outside of your organization.

Hi,

Thanks for your email, I sent it, It's a business proposal I thought to share with you, Please follow the link to view, or follow see below.

[Click here to view the document \(link expires in one week\).](#)

Let me know your thoughts when you are done.

From: Pamela S. Ulmer <Pamela.Ulmer@harrisonburgva.gov>
Sent: Wednesday, August 24, 2022 12:55 PM
To: Graham Nelson <graham@matchboxrealty.com>
Subject: email - dropbox

Graham, I received an email from you with a Dropbox link – due to security reasons as I was not expecting this, please advise if this is a true email from you and what the link contains.

Thank you!

From: Tasha Browne <tasha@matchboxrealty.com>
Sent: Monday, August 12, 2024 3:57 PM
To: Tasha Browne <tasha@matchboxrealty.com>
Subject: NewDocument Received from MatchboxRealty

WARNING: External email. Be cautious when clicking on links or opening attachments.

Good Afternoon,

As discussed, please find the updated proposal attached, Scan the QR Code to access Revised Proposed billing



Best,

Password Best Practices

- 15 characters min
- Don't reuse passwords
- Lockout after 5 failed attempts
- Should not include any parts of username
- Complexity
 - Upper
 - Lower
 - Number
 - Special Character

Most Used Passwords

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

Passphrases are better

- Easier to remember
- More convenient for end user
- Harder to crack

```
(root@kali)-[~]
└─$ john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt ./winpasswords.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (User)
qwerty        (testuser)
sanny         (Guest)
bigdog        (Administrator)
              (DefaultAccount)
5g 0:00:00:00 DONE (2022-11-11 11:26) 6.329g/s 18156Kp/s 18156Kc/s 18166KC/s      markinho..*7;Vamos!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Creating a passphrase

- Movie quotes
- Song lyrics
- Books
- Poems
- Dad jokes

Samples

- dolfeellucky?
- showmetheMoney!
- Sayhellotomylittlefriend!
- \$hakenNotstirred
- Hastalavistababy!
- !neverg0nnagiveYouup
- idonttruststairs#theyarealwaysu
ptosomething



Local Gov Cyberattacks

Business Email Compromise (2024)

Mecklenburg
@dss.virginia.gov
Amherst
Front Royal
Strasburg x2
City of Harrisonburg
Woodstock
Bridgewater
Rappahannock CJTA

Other Incidents

City of Waynesboro (ransom)
HRECC (ransom, malware)
City of Harrisonburg (website)

What can you do?

- Use passphrases
- Consult with IT/Security Team
- Practice and Encourage good cyber hygiene

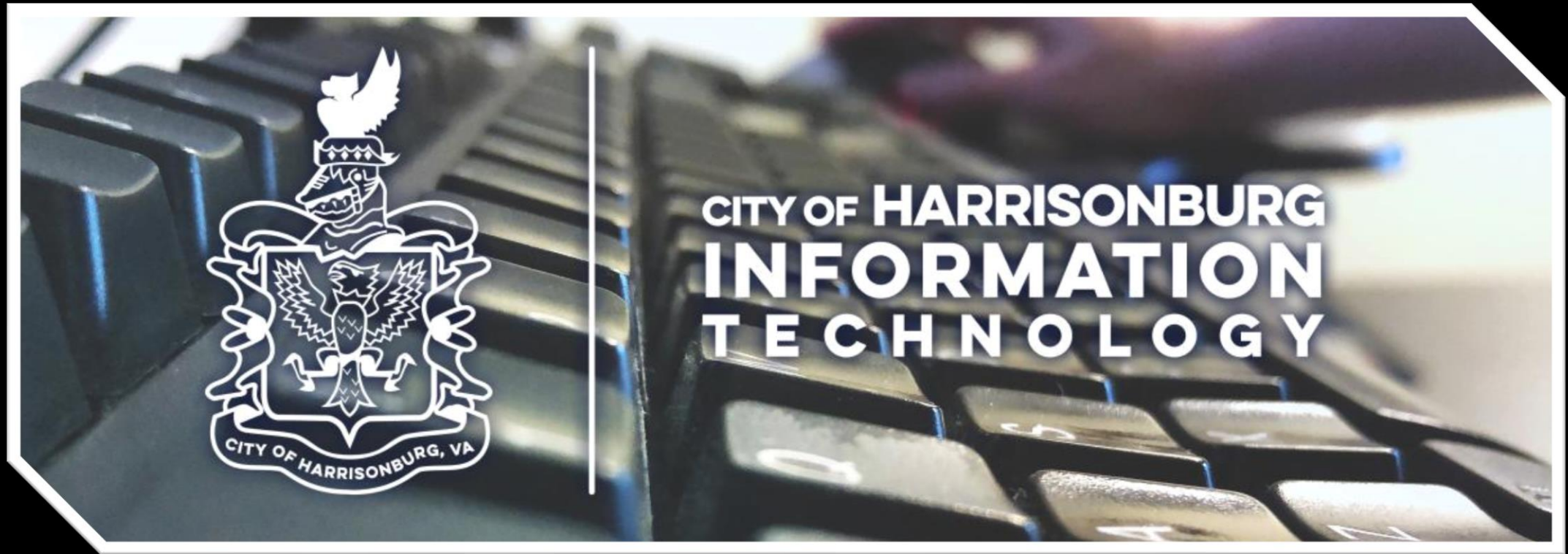


Resources

- www.cisa.gov
- www.knowbe4.com/free-cybersecurity-resource-kits



Questions



Bud Ritchie

bud.ritchie@harrisonburgva.gov

540-432-7706