COVID-19 Pandemic

PRESENT DAY Cybersecurity Challenges

Cyberstone
Secure. Compliant. Assured.

Coronavirus themed phishing attacks & hacking campaigns are on the rise

- Cybercriminals are now creating and putting out thousands of corona-virus related websites on a daily basis
- Intelligence firm RiskIQ saw more than 13,500 suspicious domains on Sunday March 15th
- More than 35,000 domains found the following day
- Mobile devices are susceptible as well

Databranch

What to watch out for

- Phishing emails claiming to contain advice on how to prevent infection, asking you to click a link or open an attachment. For example:
- Message in the body of the email states it is from the World Health Organization (WHO)
- Actuality it is the Trickbot banking trojan used to steal confidential information
- Once installed on your machine it can be used as a method to install other forms of Malware on your machine

Databranch

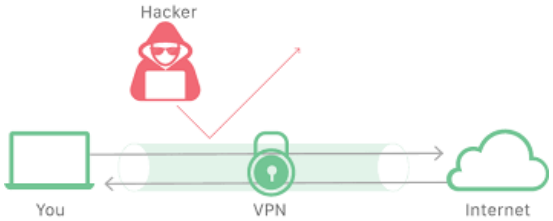
National Cyber Security Center Tips

- Many phishing emails have poor grammar, punctuation and spelling
- Is the design and overall quality what you would expect from the organization the email is supposed to come from ?
- Is it addressed to you by name, or does it refer to ‘valued customer’, or ‘friend’, or ‘colleague’? This can be a sign the sender does not actually know you, and that is part of the phishing scam
- Does the email contain a veiled threat that asks you to act urgently ?
- Your bank, or any other official source, should never ask you to supply personal information from an email.

Databranch

Teleworker Tips

- VPN: What is a VPN ?
- VPN stands for a Virtual Private Network. The purpose of a VPN is to provide you a secure network back to your office applications over the public internet
- A VPN creates a private connection or tunnel over the open internet. The idea is that everything you send is encapsulated in this private communications channel and encrypted so even if your packets are intercepted, they can't be deciphered
- Databranch can help set this up for you!



Teleworker Tips

- MFA: What is MFA?
- MFA stands for Multi-Factor Authentication. MFA is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authenticating mechanism
- **Two-factor authentication** or **2FA** is a method of confirming users claimed identities by using a combination of two different factors
- 1) Something they know, 2) Something they have or 3) something they are

Databranch

Teleworker Tips

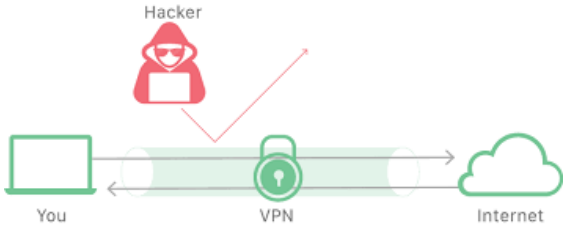
- **Two-step verification or two step authentication** is a method of confirming users claimed identity by utilizing something they know (password) and a second factor *other* than something they have or something they are
- An example of a second step is the user repeating back something that was sent to them through an out-of-band mechanism
- For example the 6-digit code that you receive from your bank when you logon to your banks mobile or online banking site

Teleworker Tips

- **Two-factor authentication** may also be accomplished via a hardware token or device. The credentials are stored on a USB device that is plugged into your laptop or desktop PC
- *DUO – YubiKey & FortiToken are some examples of hardware tokens on the market today*
- Databranch can guide you on the best form of MFA for your organization to implement

Teleworker Tips

- **Home Computer Use:** Using your home PC for teleworking provides a whole new set of challenges when it comes to security
- *Make sure your device is on a current anti-virus platform*
- *Make sure your device has a current operating system and is up to date from a software revision perspective*
- *When not is use by the person teleworking from home, make sure the users session is logged off preventing anyone else in the home from accessing business applications*
- *Databranch recommends a solution called TruGrid for our clients utilizing personal devices to work from home!*



NIST
National Institute of Standards and Technology

NIST Special Publication 800-46
Revision 2

Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-46r2

July 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

NIST
National Institute of Standards and Technology

- Plan telework-related security policies and controls based on the assumption that external environments contain hostile threats.
- Develop a telework security policy that defines telework, remote access, and BYOD requirements.
- Ensure that remote access servers are secured effectively and are configured to enforce telework security policies.
- Secure organization-controlled telework client devices against common threats and maintain their security regularly.
- If external device use (e.g., BYOD, third-party controlled) is permitted within the organization's facilities, strongly consider establishing a separate, external, dedicated network for this use.

Databranch

Cyberstone
Secure. Compliant. Assured.

If you would like more information on how to stay cyber safe during this pandemic, please feel free to reach us at:

716.373.4467 x 115

info@databranch.com

We are working and ready to help your business!

The Databranch Team