Security Concerns of COVID-19 & Work From Home (WFH)
Methods & Dangers of WFH
What methods are your employees using for WFH?

- Are they using their home devices?
- Taking work computers home
- Logging in to Terminal Servers/RDS
- Using services such as GoToMyPC
- Have cloud hosting such as MS Azure or AWS
- Are they utilizing VPN to your company networks?
Using Home PCs and Personal Laptops

- Existing Malware / KeyLoggers (Estimates are 20% Infected)
- Do the children use this device (games, etc.). Big problem.
- Set a policy for all employees to have current Anti-Virus and Malware protection on their home systems. Webroot is a good solution.
- Make sure they are using a current operating system like Windows 10. If they are using Windows 7 it is End-of-Life and vulnerable. Assist with paying for upgrade.
- Need to make sure all critical apps like Microsoft Office, Internet Explorer, Adobe, etc.. are up to date
Taking Work Systems Home

• Connecting via ethernet patch cable. Needs to be close to ISP router (cable modem). Hopefully they have some form of firewall in place.
• Connecting via wireless. Laptops no issues. PCs will most likely need to purchase a USB wireless adapter.
• Monitors and display adapters
• Do not let any other family member use device. Keep locked when not in use.
• Do not install any new applications or software on device.
How Are They Logging in to Your Network

• Remote Desktop Gateway (Secure RDP to Terminal Server or Windows Desktop)
• SSL VPN (Secure tunnel to network. Can map drives and other features but less secure.)
• GoToMyPC (Quick to setup and allow users to connect to work desktop from home devices)
• MS Azure or AWS. You can also setup a new Azure TS and connect back to your office.
• Hybrid Solutions
Technical Issues of WFH
What Technical Issues are We Seeing

• Hardware limitations – Terminal servers not having enough resources for complete remote workforce. Typically designed for a smaller percentage of team such as sales and executives.
• Bandwidth limitations – with everyone working and being entertained from home ISPs are being overloaded. Not enough bandwidth. You might also not have enough bandwidth at the office due to cable modem connections (300x20) and now the lower speeds of the upload are being maxed.
• Cloud conference systems are being overloaded.
• Phone systems (VoIP, softphones, )
• Inventories are really tight for laptops and other hardware
Email Scams
Phishing Emails

FedEx Service <details@fedex.com>
To: booking@hopefortheyving.com
FedEx delivery problem # Error ID 4900

August 13, 2012 6:54 AM

FedEx Federal Express

Unfortunately we failed to deliver the postal package you have sent on the 27th of July in time because the recipient’s address is erroneous.

Please print out the label copy attached and collect the package at our office.

Print a shipping Label

From: do-not-reply@anthem.com
Subject: To All Accounts of Anthem - Important Information

Anthem BlueCross BlueShield

Cyber Attack Against Anthem

Dear Anthem Client,

We wanted to make you aware of a data breach that may have affected your personal health information and credit card data. The data which was accessed may impact clients who made credit or debit card payments for healthcare or who got treatment during the year 2014.

Your trust is a top priority for Anthem, and we deeply regret the inconvenience this may cause. This privacy and protection of our client's health care information is a matter we take very seriously and we are working diligently to resolve the incident.

To subscribe to a free year of credit card account protection please click on the link below and follow the instructions that will be required:

Click Here To Get Your Free Year of Credit Card Protection
Hover over links and verify them!
Verify Account Activity

Barry Morgan (morg43@gmail.com)

Verify Account Activity

In an ongoing effort to protect your account, we are notifying that your email was accessed from IP address 71.65.221.46 in Raleigh, NC. If this activity authorized, please disregard this message.

To view the details, or report fraudulent activity, please contact us via the secure portal.

Google Privacy and Security Portal

Regards,
Google Account Security Team

Gmail
Malware as Voicemail
Someone just sent you a Download link

To: no-reply@pcloud.com

You forwarded this message on 3/20/2020 12:46 PM.

User [redacted] has sent you a download link for "Quote_#96286492.html".

Thank you for trusting pCloud with your files!

Best wishes,
The pCloud team
Hi!
My name is Greg Smith and I just bought a 20,000 sq ft building in Blue Ash located at 9850 Redhill Drive. It was built in the 1980’s and it has some of the original HVAC equipment currently in place. As part of a building refresh project I’m interested in converting to geothermal and I think your firm would be a perfect fit.

I have the site diagrams and architectural drawings from the previous owner that you can review. I’ve shared them on Dropbox at the link below.

Please review the information and let me know when I can meet with you for an initial consultation.

Thank you!

https://www.dropbox.com/s/sjzifwarpzycz1t/img_5672.exe?dl=0

Greg
Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear [Redacted],

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-ncov/newcases-cities.html)

You are immediately advised to go through the cases above for safety hazard

Sincerely,

CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention
Singapore Specialist: Corona Virus Safety Measures

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus. This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms: Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards
Dr [Name]
Specialist wuhan-virus-advisory
Dear sir,

Please find the attached file with the instructions on how to take this deadly virus called Coronavirus Disease (COVID-19).

This is an instruction from WHO (World Health Organization) to help fight against coronavirus.

NOTE: once received this mail, review the attached file and follow the instructions.

Please forward this mail to your family members and friends to help us reach everyone on how to fight this virus, and the instructions are very simple and affordable.

Thanks,

Best regards

Director
WHO (World Health Organization)

Dr. Tedros Adhanom Ghebreyesus
W.H.O
All,

Due to the coronavirus outbreak, {{company_name}} is actively taking safety precautions by instituting a **Communicable Disease Management Policy**. This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before {{current_date_1}}.

If you have any questions or concerns regarding the policy, please contact {{company_name}} Human Resources.

Regards,

Human Resources
Email Best Practices:

• **Beware of online requests for personal information.** A coronavirus-themed email that seeks personal information like your Social Security number or login information is a phishing scam.

• **Check the email address or link.** You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it’s obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses. Delete the email.

• **Watch for spelling and grammatical mistakes.** If an email includes spelling, punctuation, and grammar errors, it’s likely a sign you’ve received a phishing email. Delete it.

• **Look for generic greetings.** Phishing emails are unlikely to use your name. Greetings like “Dear sir or madam” signal an email is not legitimate.

• **Avoid emails that insist you act now.** Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information — right now.

• **Spoofed hyperlinks and websites.** If you hover your cursor over any links in the body of the email, and the links do not match the text, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.

• **Suspicious attachments.** An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.
Fake Websites & Apps
Fake CoronaVirus Smartphone Apps

YOUR PHONE IS ENCRYPTED: YOU HAVE 48 HOURS TO PAY 100$ in BITCOIN OR EVERYTHING WILL BE ERASED
1. What will be deleted? your contacts, your pictures and videos, all social media accounts will be leaked publicly and the phone memory will be completely erased
2. How to save it? you need a decryption code that will disarm the app and unlock your data back as it was before
3. How to get the decryption code? you need to send the 100$ in bitcoin to the adress below, click the button below to see the code
NOTE: YOUR GPS IS WATCHED AND YOUR LOCATION IS KNOWN, IF YOU TRY ANYTHING STUPID YOUR PHONE WILL BE AUTOMATICALLY ERASED
Fake Online Coronavirus Map Delivers Well-known Malware
Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV
Date: March 10, 2020

![Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE](image)

**Figure 1.** Screenshot of the malicious website “Corona-Virus-Map[dot]com” pretending to be a legitimate COVID-19 tracker.

corona-virus-map.com  ➤ Translate this page
Fake CoronaVirus Test Kit Sites
Fake Coronavirus ‘Vaccine’ Website Busted in DoJ Takedown

Authorities have cracked down on a website that claimed to give out coronavirus vaccine

Fake news buster NewsGuard is keeping busy these days, thanks to the coronavirus.
Additional Information
More than **80%** of data breaches are from *stolen* or *weak* passwords.

**Use a DIFFERENT & STRONG password for every account!**
For network passwords, we recommend long pass phrases with characters. Easy to remember and very hard to crack!

I will follow social distancing rules

Call 3 friends per day!

Save $500 more per month for retirement

Will go on more dates each month

Make it to all of kid’s soccer games

8 Character Password (4 seconds) / One above (approx. 10 seconds)
Multi-Factor Authentication

• Remote Access (RDP/Citrix)
• Exchange/Office 365
• Password Applications
• Accounting
• Client Data Applications
• Websites
  • Banking
  • Financial Advisors
  • Credit Cards
  • Medical
  • CRM
  • Any other site with sensitive data on it
Credit Freeze
<table>
<thead>
<tr>
<th>Event Type</th>
<th>Account Type</th>
<th>Dollar Amount</th>
<th>Notification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>An outgoing wire transfer exceeds $50.00 (USD)</td>
<td>PREMIER PLUS CKG</td>
<td>$50.00</td>
<td>Text</td>
</tr>
<tr>
<td>An incoming wire transfer exceeds $0.00 (USD)</td>
<td>PREMIER PLUS CKG</td>
<td>$0.00</td>
<td></td>
</tr>
<tr>
<td>A debit card transaction exceeds $50.00 (USD)</td>
<td>PREMIER PLUS CKG</td>
<td>$50.00</td>
<td>Text</td>
</tr>
<tr>
<td>An ATM withdrawal exceeds $50.00 (USD)</td>
<td>PREMIER PLUS CKG</td>
<td>$50.00</td>
<td>Text</td>
</tr>
<tr>
<td>An external transfer exceeds $100.00 (USD)</td>
<td>PREMIER PLUS CKG</td>
<td>$100.00</td>
<td>Text</td>
</tr>
</tbody>
</table>
Follow Facebook and Twitter accounts that give alerts to scams and other vulnerabilities. **SHARE WITH YOUR TEAM!**

- CDC
- OrLANtech
- KrebsonSecurity
- Federal Trade Commission
- IRS/FTC/Etc..
Stay Safe and Stay Connected
Thank You

Keith Coker, President
kcoker@orlantech.com
407-228-7290