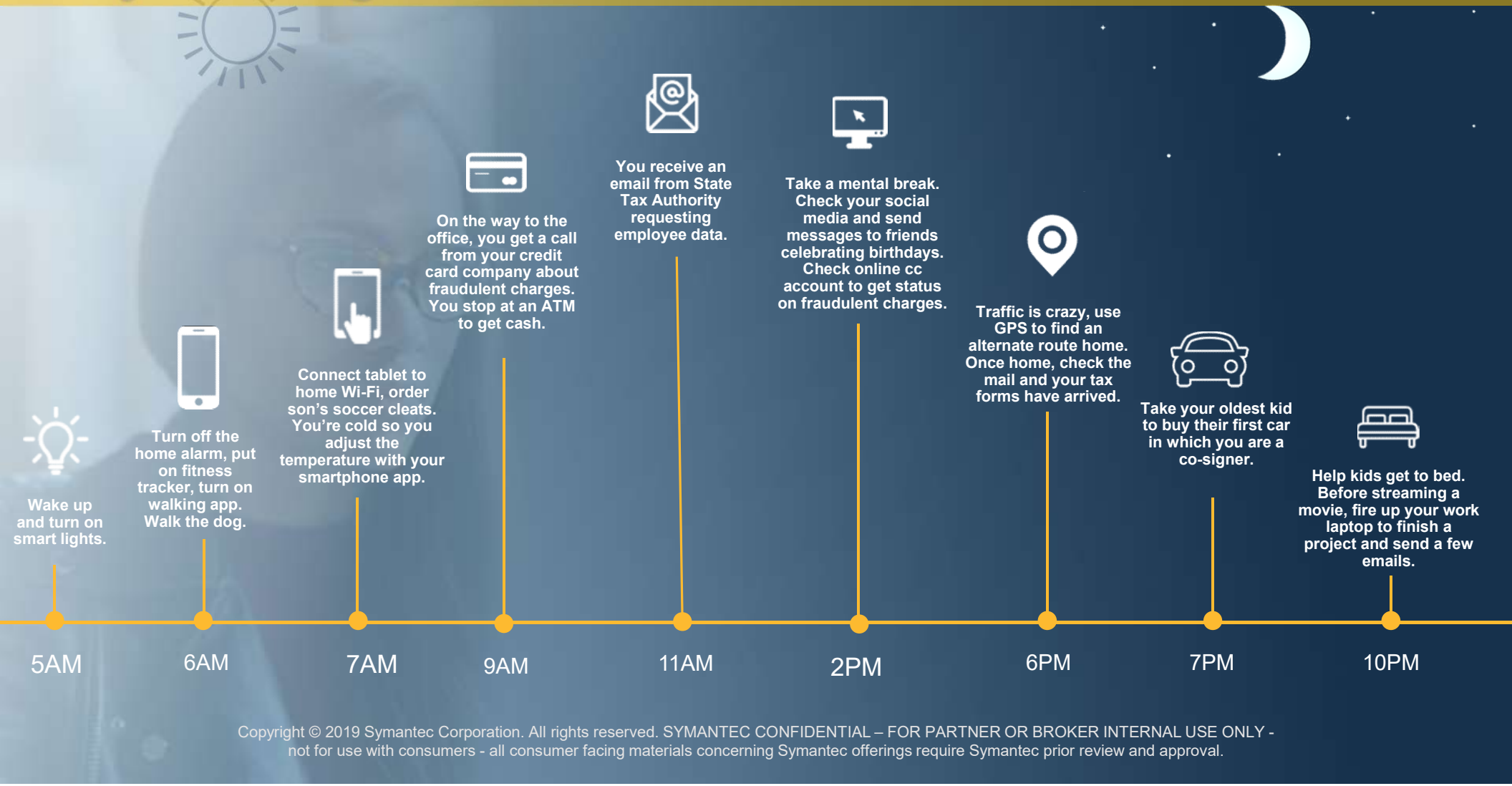
NortonLifeLock – Cyber Trends: Tips to Stay Cyber Safe in Today's World

Copyright © 2019 NortonLifeLock Inc. All rights reserved.

A Day in our Digital Lives



Copyright © 2019 Symantec Corporation. All rights reserved. SYMANTEC CONFIDENTIAL – FOR PARTNER OR BROKER INTERNAL USE ONLY - not for use with consumers - all consumer facing materials concerning Symantec offerings require Symantec prior review and approval.

Cyber Threat Landscape

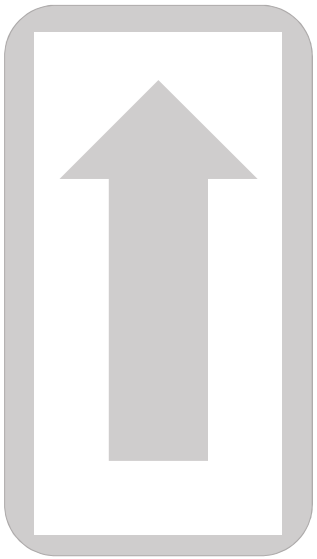
We live in a hyper-connected mobile world

One in Ten
URLs are **malicious**

48%

48% of malicious email attachments are Office files, **up 5%** from 2019

An average of **4800** websites are compromised with **formjacking** code each month



Mobile **ransomware** is up **33%** from 2019

1 in 36 mobile devices had high risk apps installed

Emerging Threats:

Creepware
Spear-Phishing
Credential Stuffing

Copyright © 2020 NortonLifeLock Inc. All rights reserved.

Protecting Against Scams in the COVID-19 Era

Phishing Scams

Copyright © 2019 NortonLifeLock Inc. All rights reserved.

Phishing Scams

- The overwhelming amount of news coverage surrounding the novel coronavirus has created a new danger —phishing attacks looking to exploit public fears about the sometimes-deadly virus.

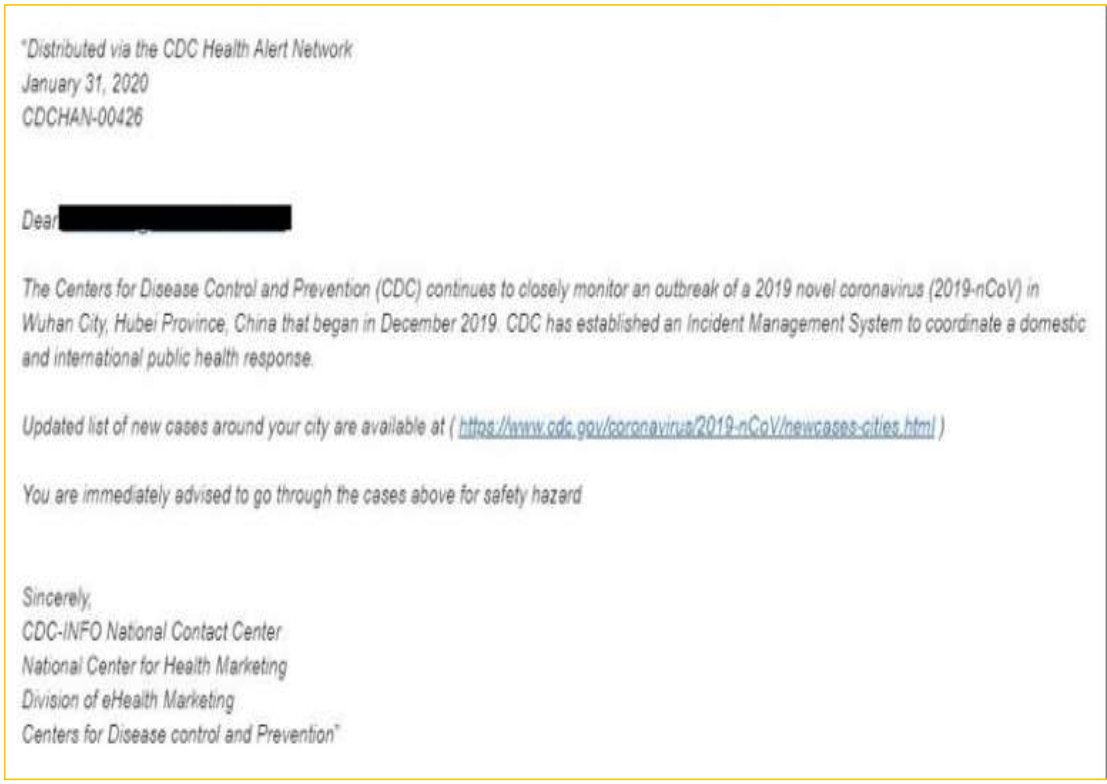
- How does it work? Cybercriminals send emails claiming to be from legitimate organizations with information about the coronavirus.

- The email messages might ask you to open an attachment to see the latest statistics. If you click on the attachment or embedded link, you're likely to download malicious software onto your device.

CDC Alert

Designed to look like they're from the U.S. Centers for Disease Control

Falsely claim to link to list of coronavirus cases in your area



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

Dear [redacted]

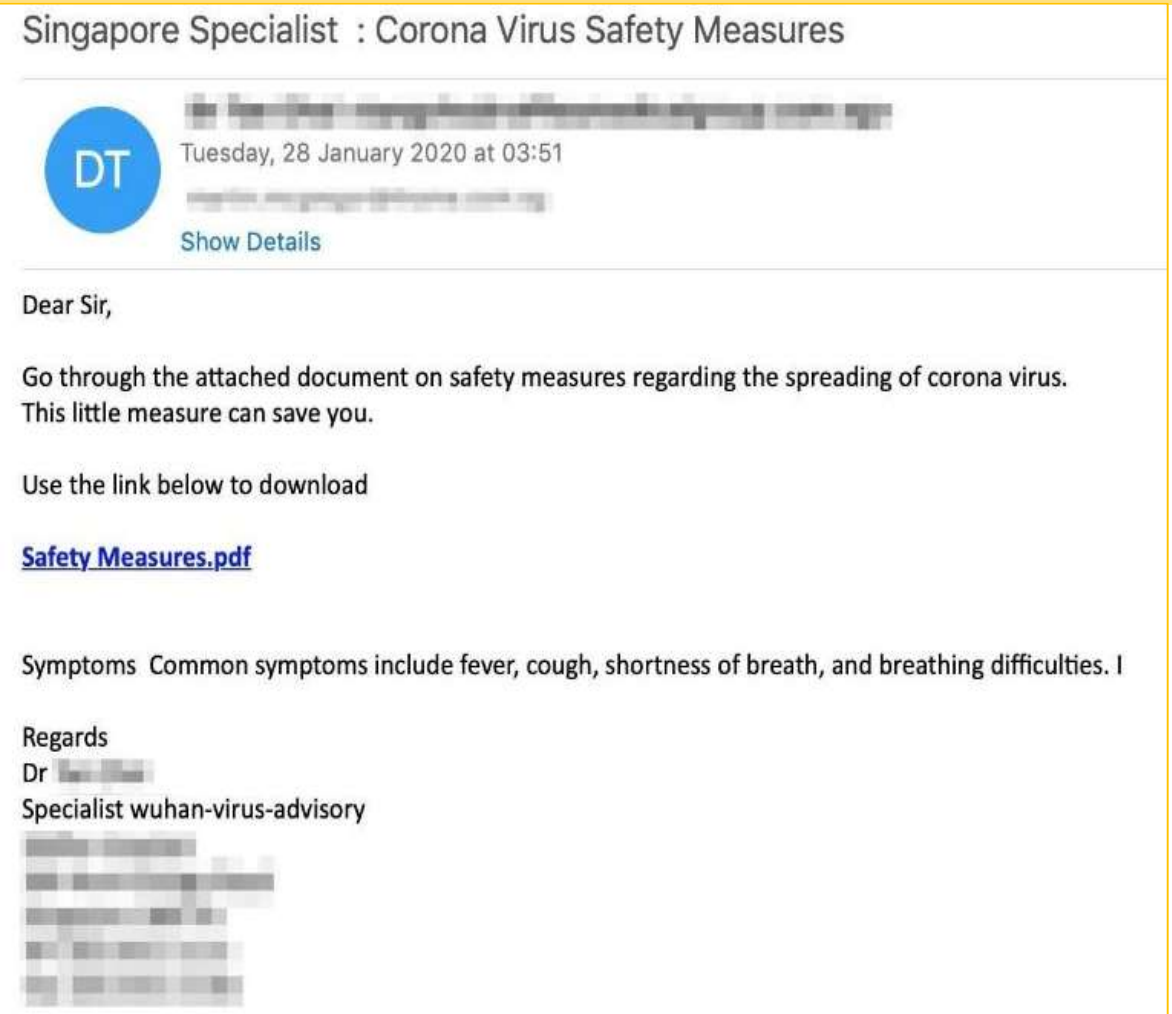
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health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

Health Advice



Singapore Specialist : Corona Virus Safety Measures

DT

[redacted]

Tuesday, 28 January 2020 at 03:51

[redacted]

Show Details

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. I

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

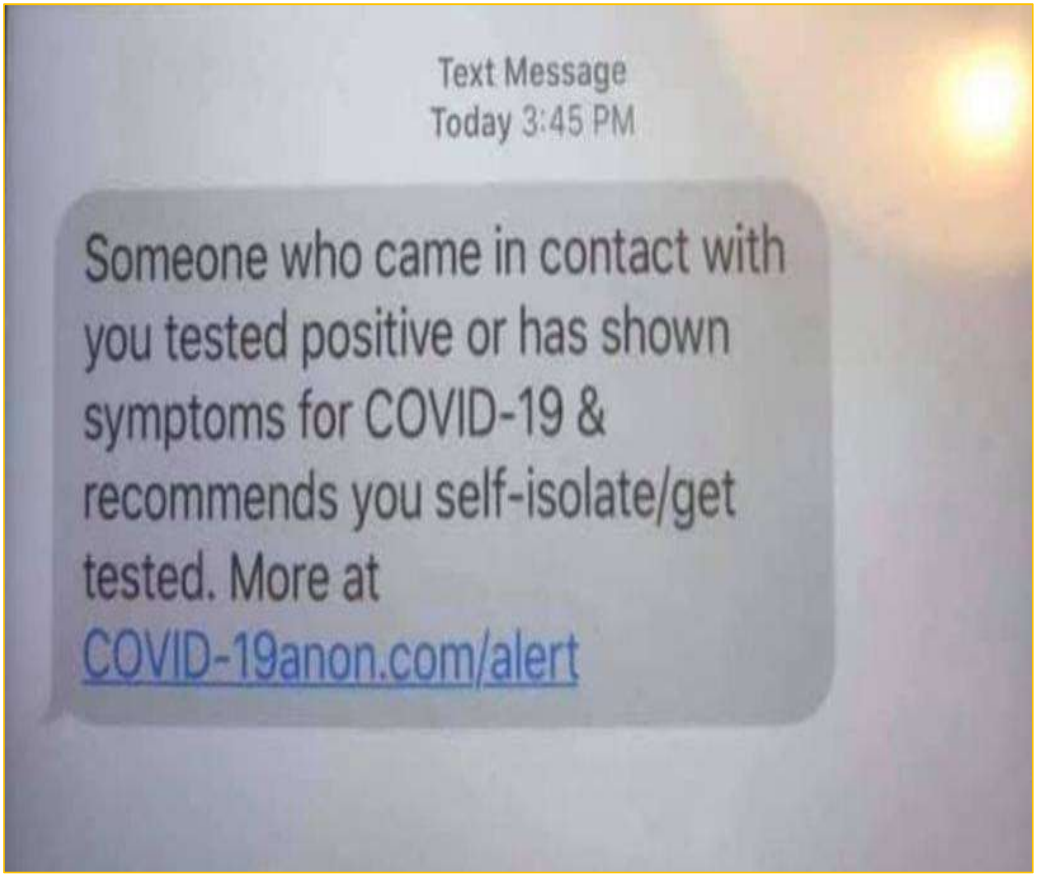
Offer purported medical advice to help protect you against the coronavirus

Provides links to download “Safety Measures”

Text Message Malware Link

Un-prompted, no identification of sender

Contains a malicious link



Workplace Policy Emails

Specifically target workplace email accounts

Usually contain a link to fake company policy that contains malicious software

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]]**.

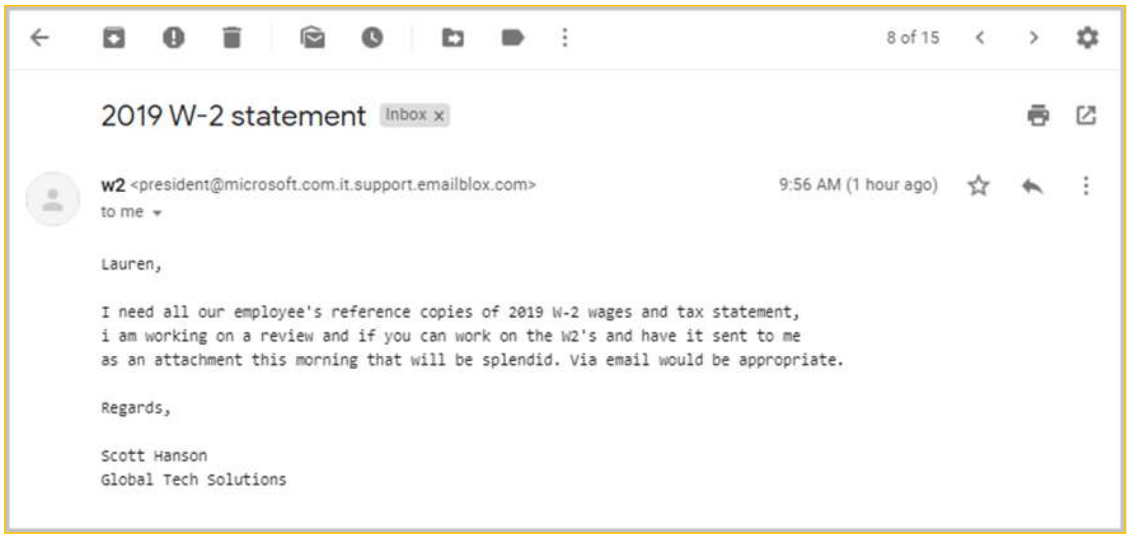
If you have any questions or concerns regarding the policy, please contact [[company_name]] Human Resources.

Regards,
Human Resources

Business Email Compromise

Often enhanced by spear-phishing

May contain requests for confidential information



Business Email Compromise

Hello Emily,

Please see the below attached invoice for payment, we are ready to proceed with shipping next week, please ensure the invoice is paid in time.

Shipping charges are additional.

FFH Concept GmbH

Invoice Due:01/27/2020
873/FFHC

Amount Due: 388,700.11

Dear Customer :

Please see the attached Invoice. Wire transfers may be directed to:

FFH Concept GmbH.
Address: Alexanderpl. 7 , 10178 Berlin Germany

BANK DETAILS:

Bank name: GLS Gemeinschafts bank eG

Account name: FFH CONCEPT GmbH
Bank Address: Chrisstr .9. 4474 Bochum
[redacted]

Shark Tank's Barbara Corcoran targeted by spear-phishing business email scam

Resulted in ~$400K compromise

Tips to Recognize and Avoid Phishing Emails

Beware of online requests for personal information

Look for generic greetings

Check the email address

Avoid emails that insist you act now

Watch for spelling and grammatical mistakes

Hover over included links to ensure accuracy

Unemployment And Stimulus Check Scams

Copyright © 2019 NortonLifeLock Inc. All rights reserved.

Unemployment Scams

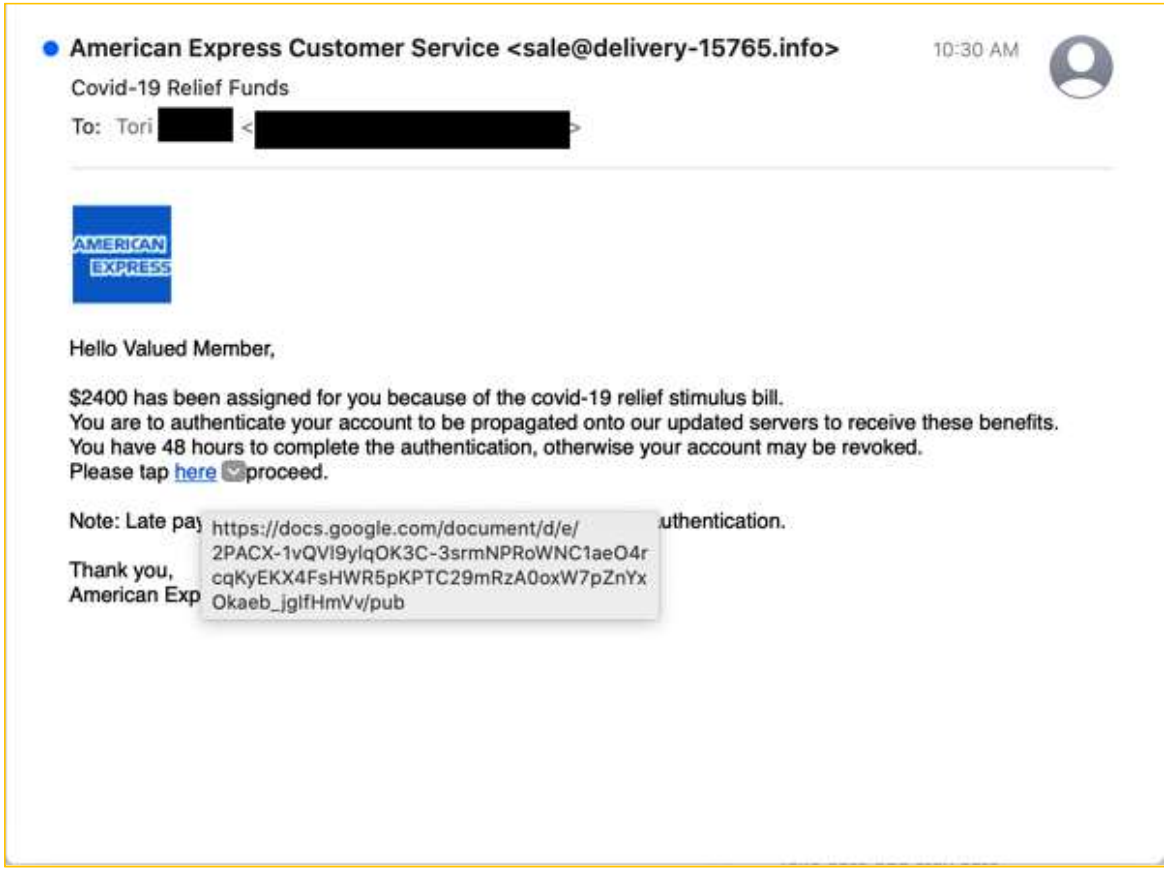
- Newly idled Americans have filed millions of unemployment claims during the COVID-19 outbreak. Calls to state employment insurance services have at times overwhelmed phone lines and websites. That's created opportunity for fraudsters.

- How? In some cases, scammers are pretending to represent government entities. Their goals include stealing claimant's benefits, money, and personal information to commit crimes such as identity theft and other frauds.

Stimulus Scam

May attempt to spoof a bank or financial institution

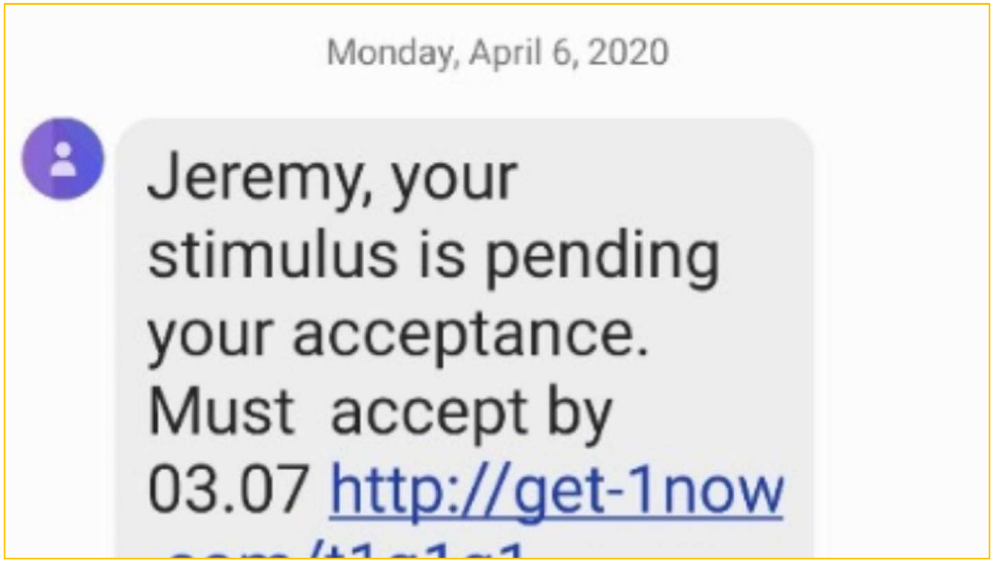
Beware requests demanding urgent action or response



Stimulus Scam

Texts can be personalized to recipient or current events

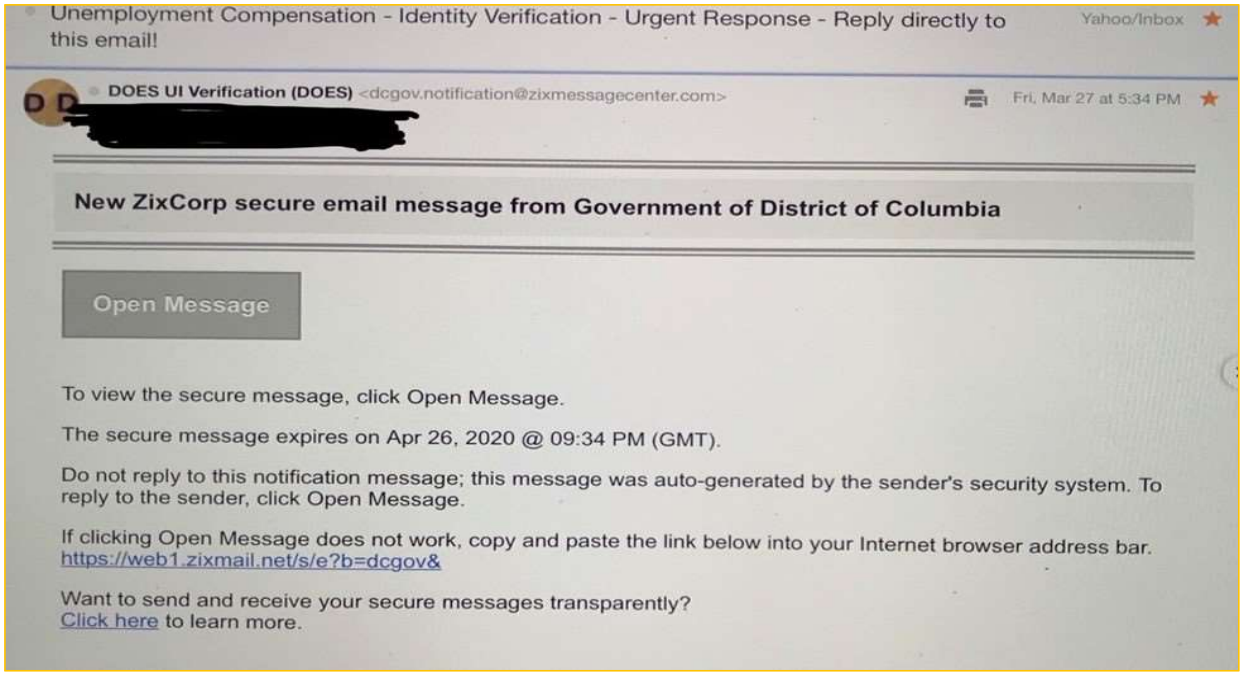
HELP is common short text code to determine more info about sender



Unemployment Scam

Often impersonates government body

Secure mail redirects to mask information collection



Common Unemployment Scams

Phishing – Emails from “Unemployment Assist” with subject lines that read “ID Eligibility Requirement” or “Verification Required”

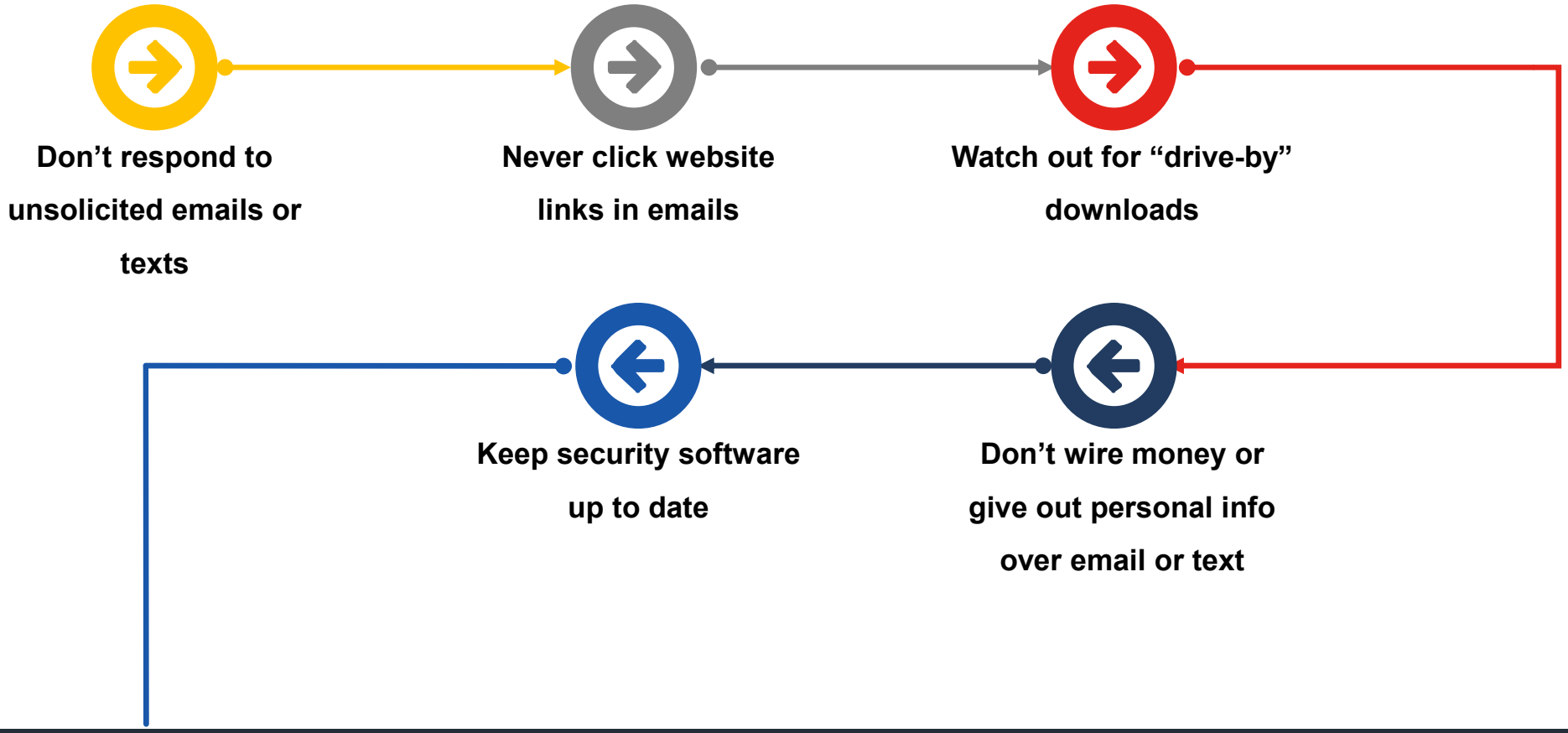
Debit and Direct Deposit Card Scams – State specific, insists that recipient apply for one of the unemployment cards

Fake Phone Call Scams – Phone and text messages that indicate that unemployment benefits account was suspended, call another number to resolve

Jobseeker Scams – Pretend to be employers to collect information or trying to get money

Fake Website Scams – Sites that indicate they will help you file for unemployment benefits, or file on your behalf

Tips to Avoid Unemployment-Benefit Scams



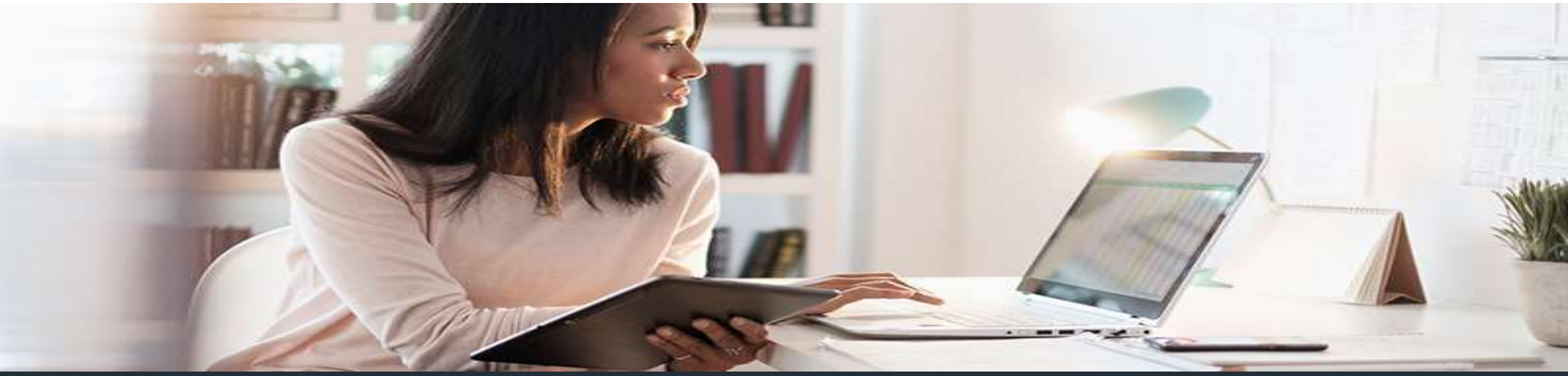
Securing a Remote Network

Copyright © 2019 NortonLifeLock Inc. All rights reserved.

Working From Home

- Companies such as Apple, Google, and Microsoft have announced they are allowing staff to work remote to help protect against the coronavirus.

- If you decide to work remote, it's a good idea to keep cybersecurity in mind. That means protecting your devices and data, just like you would in the workplace.

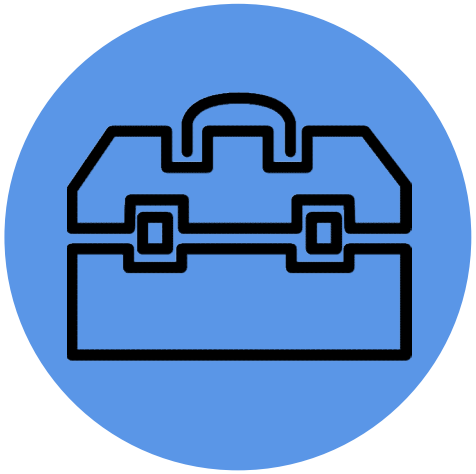


Working From Home

Keep close contact with your employer

It’s smart to stay on top of company communications. Your inbox might contain emails about policy changes ranging from work hours to travel. Your employer might consolidate coronavirus-related information on the company intranet. If you have questions, ask.

Working From Home



Use what's in your company's tech toolbox

Companies often have tech tools that can help keep you cybersafe when you work from home. That might mean you do your work on company-supplied laptops and mobile devices. They likely include firewall and antivirus protection, along with security features like VPN and 2-factor authentication.

Working From Home

Control the impulse to improvise

Employees often work in teams, and that can mean using collaboration tools like instant-messaging platforms and video-meeting rooms. If a tool isn't working right, you might be tempted to download a substitute. Don't do it. You could inadvertently introduce a software program with a security flaw — and that means someone unauthorized may be able to access company data, or any personal data you have on that device.

Working From Home

Stay current on software updates and patches

You might get reminders that software updates are available for your computer, laptop, tablet, or mobile device.

Don’t wait. Update. Also, keep in mind you can configure your devices to update automatically.

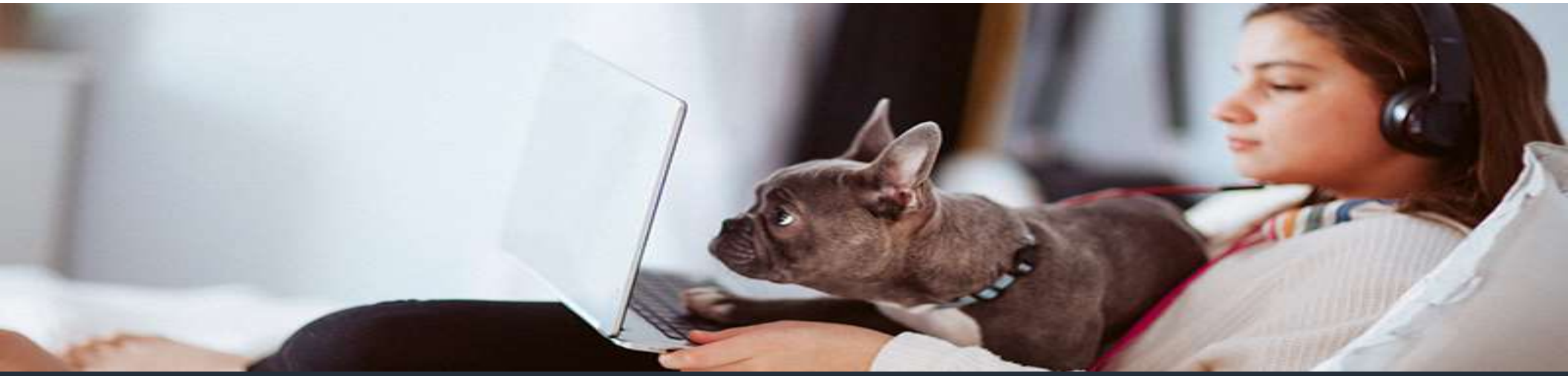
Protecting Kids Online

Copyright © 2019 NortonLifeLock Inc. All rights reserved.

Protecting Kids Online

- Many families spend a lot of time at home — more so, recently, due to health concerns related to COVID-19. At-home time often translates into more hours spent online. For kids, that might involve school, homework, socializing, entertainment, and gaming.

- But not everything online — or every online activity — is well-suited for kids and teens. What can you do? You can help monitor online time and activities in various ways. You can set guidelines and check in with your kids to make sure they're followed. You might also consider a parental-control app to help you manage some of these tasks.



Protecting Kids Online

Schedule screen time limits for kids and devices

Monitor what your kids are doing online

Set rules about using social media

Stay on top of information shared online

Limit access to websites

Keeping tabs on what your kids do online requires effort. Even so, it’s a good idea to take steps to monitor who they're talking to, where they go, and what they consume and download.

It's also a good idea to periodically discuss online citizenship and whether your kids still agree with the house rules. The goal is helping to keep your kids safe online while building safe and smart online habits.

If you find yourself spending more time with your kids at home — by choice or necessity — you’ll be glad you took the time to guide them online.

Video Game Scams

Copyright © 2019 NortonLifeLock Inc. All rights reserved.

Video Game Scams

- Games have a robust economy both in and out of the games themselves. In-game currency, in-game purchases, real-world currency stored in wallets and the games themselves are all lucrative assets, and they are enticing targets for scammers and cybercriminals.

- Cyberthieves have already unleashed a host of scams focused on the stimulus checks the federal government is providing to help lessen the economic impact of the pandemic. And because scammers have always targeted video game players, it wouldn't be surprising to see the number of gaming scams rise as more people, confined to their homes, log on to their favorite games.

How are Gamers Targeted

Fake Games – Generally fake mobile versions of popular online games that install malware on the users device

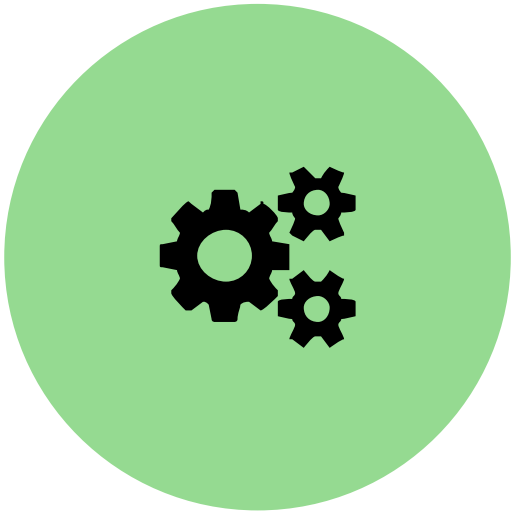
Phishing – Emails to gamers asking them to confirm their password, or login to a website infected with form-jacking malware

Takeover Scams – Malware that takes advantage of the poor security of many gaming platforms to steal credentials

Third Party Websites – Tricks gamers into visiting third party websites to download game enhancements, but compromises provided info

IP Address Compromise – Used to identify your real info to commit physical attacks such as doxing or swatting

Tips to Avoid Compromise



- **Don’t respond to emails or direct messages from Discord, Twitch, or Steam requesting info**
- **Be cautious towards password scams**
- **Use two-factor authentication whenever possible**
- **Install and use a VPN when playing games that can expose your IP address**

Telemedicine Safety

Copyright © 2019 NortonLifeLock Inc. All rights reserved.

Telemedicine Safety

- The recent boost in virtual doctor visits due to social distancing brings new worries of privacy. How secure is the information shared during these online visits with healthcare providers? Can cybercriminals steal your personal health or financial information?

- Fortunately, there are steps you can take to help protect your privacy while using video conferences to discuss medical issues with your doctors and other healthcare providers.

Telemedicine Safety

As early as February, virtual doctor visits accounted for 1% of physician visits. **Today, more than 80% of network patient visits are being moved to telemedicine platforms**. Hackers try to exploit these networks, monitor keystrokes, and intercept documents sent between doctors and patients due to the high value of medical records.

Ask if your medical provider saves your video sessions

Use video-conferencing services that rely on encryption

Be careful what information you send in emails or text messages

Ask if your medical provider shares your medical information with third parties

Why We Protect Employees and their Wellness

We believe that everyone has the right to explore this amazing yet increasingly complex digital world.

Everything we do is focused on protecting your employee and their *financial and personal wellness.*

Together Norton and LifeLock are redefining what it means for your employee to be safe in the digital world.

We securely connect People, Information & Things everywhere.

Thank You!

Copyright © 2019 NortonLifeLock Inc. All rights reserved.