

The impacts of COVID-19 have forced the nation to make a shift in the workplace. Aside from essential employees, many companies have restructured the workplace with an emphasis on working from home (WFH). As such, employers as well as employees need to be aware of best practices for working remotely. If the IT side of a business is configured correctly and employers and employees follow appropriate security requirements, telecommuting can be safer and more reliable and ensure data security.

Moving with short notice at a rapid rate during this time of demand and uncertainty from a trusted office workplace to working remotely can bring a variety of cyber security risks. Improper WFH procedures can lead to data breaches and a host of other issues. It is vital that both employers and employees take proper precautions to limit risks of any intrusion within company network systems and compromise of user endpoints.

This article will review these and other WFH matters:

- Using home PCs, laptops and devices
- Using work systems (computers and laptops) at home
- Accessing your network
- Having technical issues
- Knowledgeable in how to recognize email scams
- Familiar with VoIP phones and fake voicemail messages
- Microsoft Azure and Office 365
- Adept in identifying fake websites and apps
- Using secure and different passwords and/or 2FA or MFA

Here are things to consider and guidelines to follow that will help you, your business and your workforce when working outside the office.

## Using Home Systems

If your workforce is using their personal PCs and devices, a company can be at risk due to the following:

- Home systems could be infected with existing malware and keyloggers. (Estimated 20% are infected.)
- Children and other family members using devices with infected games, falling for scams, downloading malware, etc. (Big problem!)
- Lack of reputable antivirus and malware protection on their home systems. ([Webroot](#) is a good solution.)
- Operating systems lacking current updates and security patches. Make sure to keep your operating system (Windows 10) updated and patched. If they are using Windows 7, it is End-of-Life and that means vulnerabilities are increasing daily. These systems should be upgraded or replaced ASAP!
- Critical apps that are not up to date, such as Microsoft Office, Internet Explorer, Adobe, etc.

## Using Work Systems (At Home)

If your workforce is using company PCs and devices, they should do the following:

- For work PCs, they will most likely need to connect the system with an ethernet patch cable. They need it to be close to the ISP router (cable modem), or they will probably need a long patch cable. Hopefully they also have some form of firewall in place.
- If they bring their PCs home without the monitors, they could run in to issues connecting them. There are several different video connections, and they need to make sure the connections match. They can also purchase adapters if needed, but these can be hard to find due to short inventories. The best thing is to bring the monitors home along with their work PCs.

- If connecting wirelessly, laptops should be able to connect to their home wireless network. PC users will most likely need to purchase and use a USB wireless adapter.
- They should not let any other family member or person use their work devices. When not in use, keep the devices locked and password protected.
- Do not install any new applications or software on the devices unless absolutely needed.
- Turn off the device used for work when done for the day. This will terminate any remote connections to the workplace and reduce the chance of that machine being compromised.

## Accessing Company Networks

Here are different ways to access a company's network:

- Remote Desktop Gateway (Secure RDP to Terminal Server or Windows Desktop).
- SSL VPN (Secure tunnel to the network. Can map drives and other features, but it is less secure without proper precautions in place. Think of a home PC with malware being connected directly to your servers at work). (Can also RDP to desktop through the SSL VPN).
- [GoToMyPC](#) (Quick to setup and allows users to connect to work desktop from home devices.).
- MS Azure or AWS Cloud Hosting of servers. You can also setup a new Azure Terminal Server and connect it back to your office via VPN.
- Cloud file sharing services, such as SharePoint, Box or Egnyte.
- Hybrid solutions to share resources across the network.

## Potential Technical Issues

These are technical issues that remote workers might experience during this pandemic:

- Hardware limitations – Terminal Servers typically are not configured with enough resources for a complete remote workforce. They are typically designed for a smaller team, such as sales and executives. This could result in decreased performance with these servers.
- Bandwidth limitations – With the number of people working and being entertained online from home, ISPs are being overwhelmed. Basically, there is not enough bandwidth to handle these increases and performance can be degraded during the peak times, such as early to mid-morning. In addition, there might not be enough bandwidth at the office due to cable modem connections. For example, a 100MB download x10MB upload with the lower upload bandwidth causes the thresholds to be maxed frequently and can cause dropped connections and/or slow performance.
- Cloud conference systems (Zoom, etc.) are being overloaded.
- Phone systems (VoIP, softphones) are having issues working properly with voice quality due to bandwidth issues.
- Inventories of laptops, headsets and other hardware are scarce.

## Social Engineering Scams

Please be aware of recent social engineering scams. A couple of the most dangerous are as follows:

- The first is where scammers call your main number to see who will answer. They will ask if you have inhouse or outsourced IT support. If you say you have it outsourced, they will then ask who it is, and if you are happy with their support. Once you give them this information, the rest of the conversation is for making it feel like it is a legitimate call. Once you have hung up, the scammers will go to the IT vendor's website (*using OrLANtech here as the IT vendor*) and LinkedIn pages and look for the names of their

engineers. Next, they will go to your website or LinkedIn page and look for the names of some of your employees. They will wait a few days and then call back and ask for one of your employees and state they are one of OrLANtech's engineers. Since they have legitimate names from both OrLANtech and your company, they trick you into forwarding the phone call. Once they are talking with your employee, they will state OrLANtech is having issues with the security and monitoring agents on their device and request your employee to go to a website to allow OrLANtech to get back into their system and re-download the agents to correct the problem. This is a scam, and if the employee complies, he/she has just allowed the hacker to take full control over their device and get hold of their network credentials and any other sensitive information they can obtain. Depending on the scammer's access back to the servers, it could turn into a severe ransomware type of event.

- The next social engineering scam is similar, but the scammers call up one of the users working from home and states they are from Apple tech support and are detecting that person's home router has been breached. If the user questions their legitimacy, they tell them to go to Apple's support page and make sure the caller ID on his/her phone matches the tech support number, which it will since it has been spoofed. They will then ask the user to go to a website which might have the name Apple in it (apple-tech-support.com, etc.) to allow them to get in and correct the user's router issues (typically for free). Once the user does this, they have just given the hacker complete access to their device.

Our advice for both these types of scams is to hang up and call back the number for these companies. Please make sure your entire team knows not to allow any tech support company to assist them without hanging up first, and then calling back the numbers listed on their website and verifying the call.

### Emails Scams

Phishing emails are more difficult to spot than ever, and scammers are targeting small and medium-sized businesses (SMBs). They are imitating large industries that typically only have a few major players in the market, such as delivery services: UPS, FedEx, USPS; cell phones carriers: Verizon, Sprint, AT&T; and healthcare insurance companies: Anthem, United Health Care, Humana, etc. to fool users into opening them.

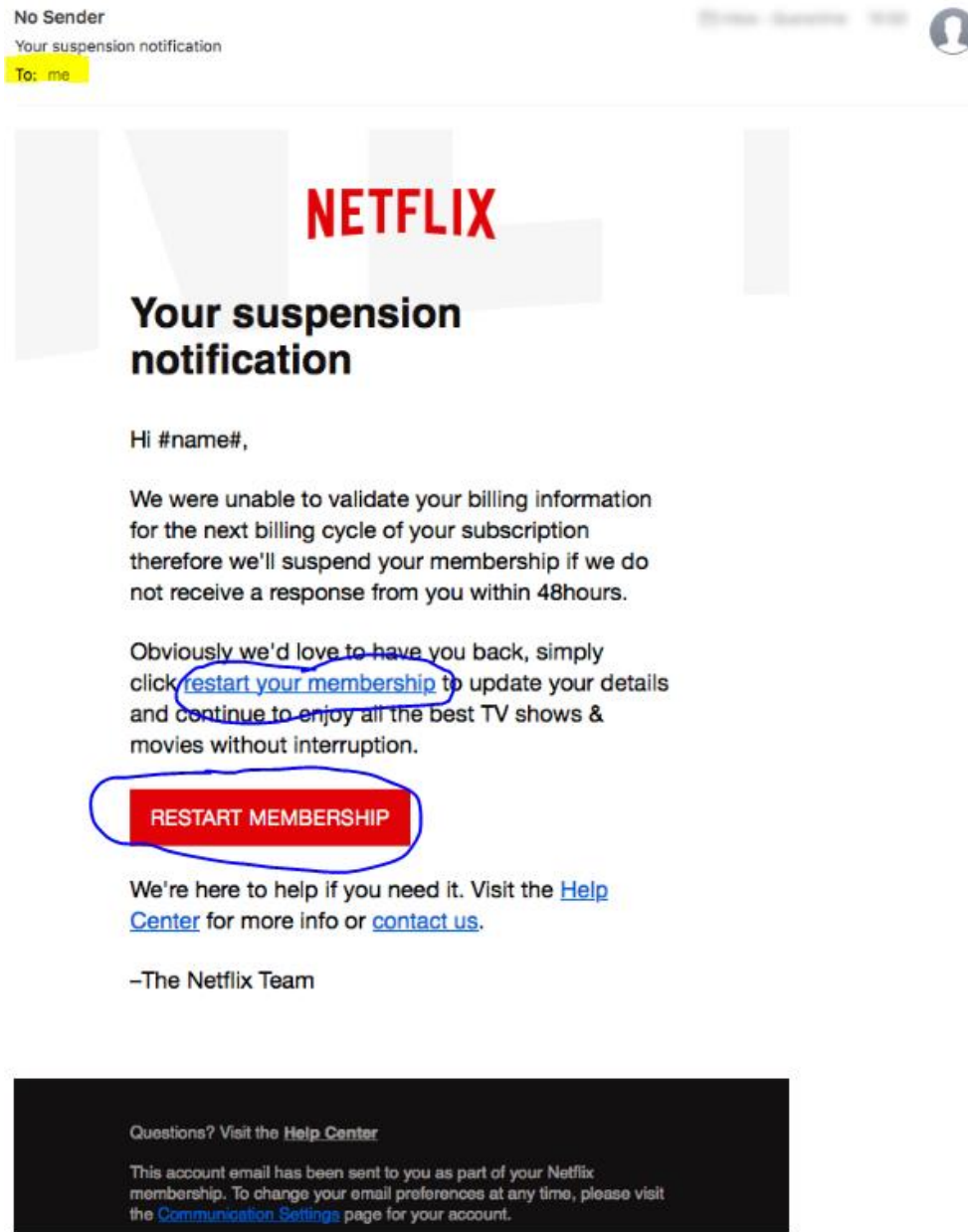
Here are ways to spot email phishing scams:

- Urgent requests
- Emails that state your account is about to expire
- Banks withdrawal notices
- Notices impersonating companies you do business with (these may include logos)
- Unknown Attachments
- Impersonal greetings
- Notices for "You've been paid" or "There's a billing problem"
- Virus alerts
- Contest winner

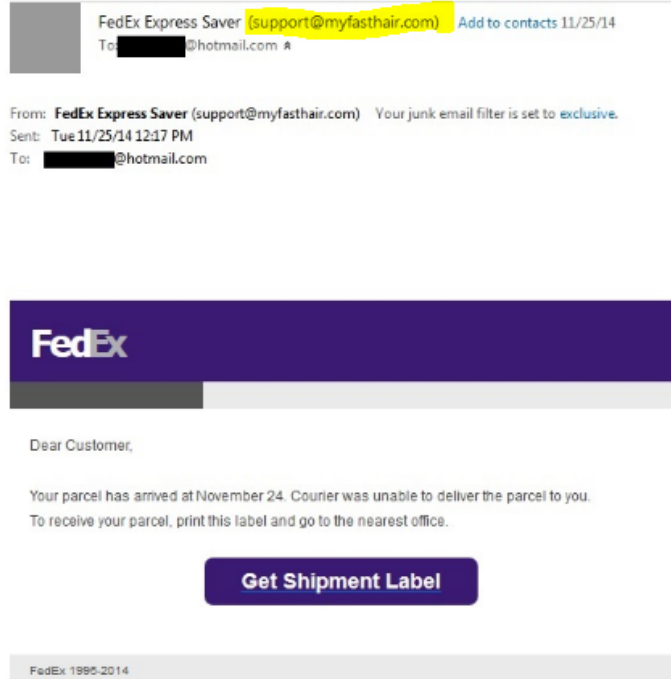
The following pages are Email Best Practices to use in detecting fraudulent emails. Please review them carefully to be better prepared because email scams are becoming more frequent and dangerous.

## EMAIL BEST PRACTICES

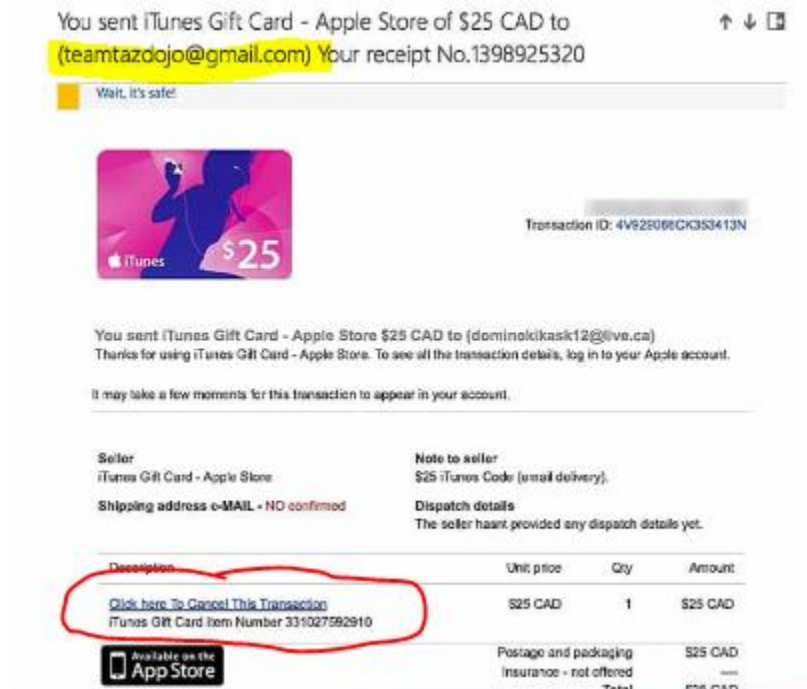
**1.) Personal Information** – make sure to verify any email request that asks for your *personal information* and/or *login* information. You can see in this example the “recipient” field shows a placeholder instead of the victim’s name. In addition, always hover over the link to verify the URL. In this case, the button goes to the same place.



**2.) Email addresses and links** – pay attention to the “from” email address to verify it is from a legitimate sender. If you were able to click on the “Get Shipment Label,” it would take you to a fake website where your credentials would be revealed.



**3.) Verify links** – hover over links and verify them before clicking. This one is not only from a suspicious sender, but if you could hover over the link, you would see it would take you to a site full of malware.



## 4.) Spelling and grammatical errors – delete any email that has errors such as these.

From: MSteam-Outlook Message Center <[no-reply@office365protectionservices.co.uk](mailto:no-reply@office365protectionservices.co.uk)>  
Sent: 19 September 2018 11:44  
To: Bob Smith <[Bob.Smith@Company.com](mailto:Bob.Smith@Company.com)>  
Subject: Account Verification

**Fake domain**

This mail is from a trusted sender.



### Threat

We're having trouble verifying your Office365 account: [Bob.Smith@Company.com](mailto:Bob.Smith@Company.com) on our server, most features will be turned off.

To help prevent account malfunctions, please log into your account portal to verify your account.

### Spelling mistakes

[SIGN IN TO MICROSOFT ACCOUNT PORTAL](#)

**Note :** Outlook will automatically fix your account after this process on the microsoft server and all account features will be turned back on

Thanks for using office365 , we hope to continue serving you.

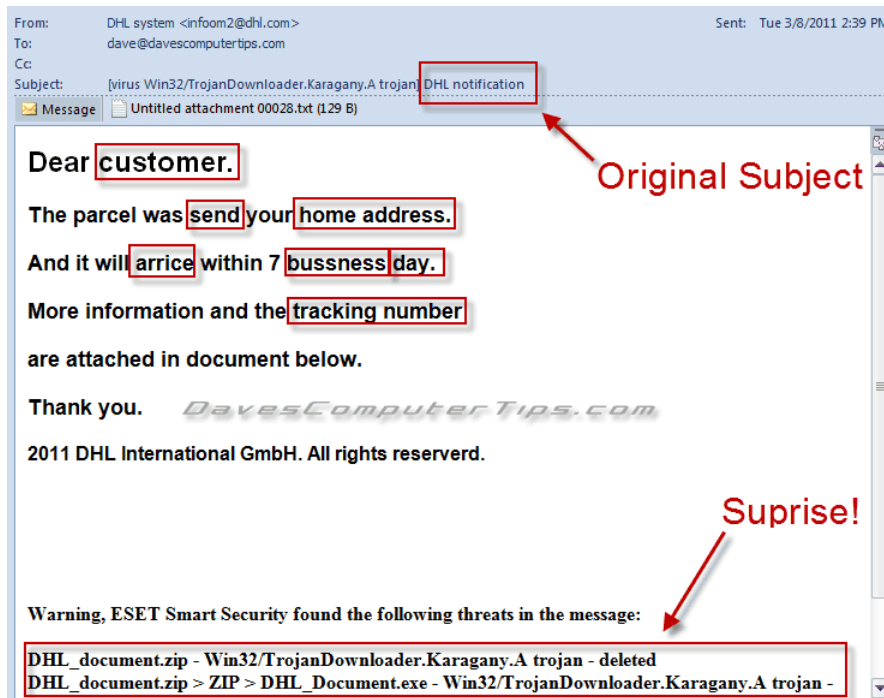
Microsoft Corporation  
One-Microsoft Way Redmond  
WA, 98052

### Grammatical errors

All Right Reserved | Acceptable Use Policy | Privacy Notice

### Fake email signature

## 5.) Suspicious attachments – there are many clues in this example that the attachment is malicious. Do not go any further. Delete the email immediately.



From: DHL system <[infoom2@dhl.com](mailto:infoom2@dhl.com)> Sent: Tue 3/8/2011 2:39 PM  
To: [dave@davescomputertips.com](mailto:dave@davescomputertips.com)  
Cc:  
Subject: [virus Win32/TrojanDownloader.Karagany.A trojan] DHL notification

Message: Untitled attachment 00028.txt (129 B)

Dear customer.

The parcel was send your home address.

And it will arrive within 7 bussness day.

More information and the tracking number are attached in document below.

Thank you. *DavesComputerTips.com*

2011 DHL International GmbH. All rights reserverd.

Warning, ESET Smart Security found the following threats in the message:

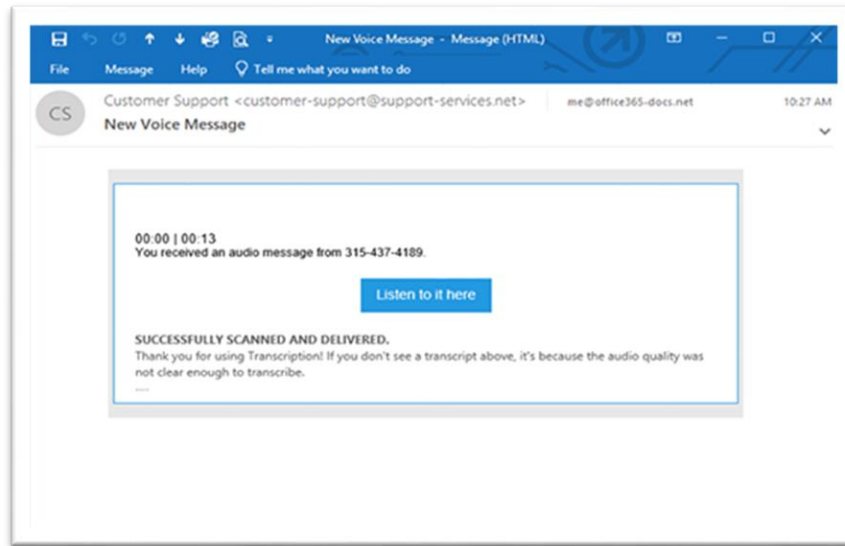
DHL\_document.zip - Win32/TrojanDownloader.Karagany.A trojan - deleted  
DHL\_document.zip > ZIP > DHL\_Document.exe - Win32/TrojanDownloader.Karagany.A trojan -

**Original Subject**

**Surprise!**

## 6.) VoIP phones and fake voicemail messages

Be careful of voicemail-to-email fake emails containing malware. They should always be in the same format. Do not open if they look different. Your VoIP vendor should be able to setup a keyword in the subject line for your team to verify it is legitimate.



## 7.) Fake Websites

There are thousands of them, and these basic tips will help you identify them to protect yourself from this growing threat.

Websites

- Unusually low prices
- No reviews
- Misspelled words and grammatical errors
- No SSL certificate on URL
- No SSL certificate on payment page
- No company/vender's address(es)
- Terms and conditions are obscured, missing or unfavorable

## 8.) Fake Smartphone Apps


The best way to identify that an app is fake is to find the developer's name below the app's name, and then do a search. It should give you valid information about the developer, like a website. If the developer has created multiple apps, then they are more likely to be legitimate. The number of downloads and app ratings gauges trustworthiness. For example, if an app has been downloaded millions of times, it is more likely to be safe but not always. Also, you can always do a search on Google with the app's name to see if it is legitimate. For example: "Is Tik Tok legit". Even though this has been downloaded millions of times the search will show you several articles of security concerns for you to make an informed decision on whether to download or not.




In summary, WFH requires that you keep your company and your clients/customers secure. It is a matter of connectivity and strict security. Using proper connectivity with home and/or work devices, providing training, support and regular screening, remote workers can help ensure company-wide data security. Lastly, we have included the infographic below on the importance of password best practices due to how critical it is for your team to practice these.

For more information on how to implement and maintain a secure remote workforce, [contact us](#) today.


### Using strong passwords to protect your security and identity




The use of strong passwords are essential in preventing unauthorized users access to your computers, devices and online accounts. Simple and commonly used passwords can allow intruders to easily gain access and take control of computing devices and data.




Use a startup password on all PCs to boot them. Turn on password/PIN protection or fingerprint recognition on all mobile devices.



Use two-factor and/or multi-factor authentication for important websites, such as financial institutions, email, e-commerce, etc. It adds an additional layer of security as a supplement to your username and password to improve your online account security.



Change the manufacturer's default password that are preinstalled on all computing devices.



Consider using a password manager to keep track of your passwords. These passwords are longer than eight characters, hard to guess and contain a mix of characters, numbers and special symbols. A trusted password manager can create, store and work across your desktop and mobile devices. Make sure the "master" password is a strong one.

## Amount of Time to Crack Passwords

"abcdefg" 7 characters	🕒 .29 milliseconds
"abcdefgh" 8 characters	🕒 5 hours
"abcdefghi" 9 characters	🕒 5 days
"abcdefghij" 10 characters	🕒 4 months
"abcdefghijk" 11 characters	🕒 1 decade
"abcdefghijkl" 12 characters	🕒 2 centuries