Annual Security Awareness Training Program

Cyber Awareness Programs can dramatically reduce the risk of cybercrime in your organization.

The best learning occurs through a combination of different learning delivery types, as well as interactive engagements. With workers more transient than ever, it is more challenging for Enterprises to secure each individual users, and therefore it is incumbent on users to be able to mitigate the cyber risks that are presented on a daily basis.

Digital Beachhead's Annual Security Awareness Training Program weaves in the following User Engagement Activities to create an effective Cyber Learning Model, measurably reducing risks for users and their employer. The activities consist of:

- Introductory and Overview Communications
- Review of Policies and Corporate Documentation (optional)
- Review of Phishing Simulation Methodology and Foundations
- Gamified learning experience in Student Portal
- Optional 'Phish Button' installation in Email Browser
- Monthly Training Activities and tracking within Student Portal
- Monitoring of Dark Web Alerts, and User Engagement to remediate any threats
- Monthly Phishing Simulations to assess continued ability to identify phishing emails

Optional Kickoff/Communication Message: A kickoff or Communication is a very important part of users understanding and embracing the Security Awareness Training process. We have created templates to customize the message to your business needs. Awareness Training kickoff messages can be sent from our Administrative Portal, or copied and sent from your internal email.

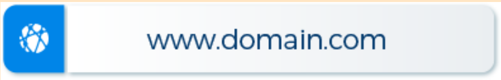
Our Phishing Simulation Methodology:

The training campaigns send simulated phishing emails to selected employees in an effort to understand how the employees behaved, and interacted (or did not interact) with emails that may have been malicious in intent. In all simulated phishing emails, there are opportunities for Organization users to identify that the subject training email is not authentic, and may be hazardous. Those characteristics are:

1. Sender Name is manipulated to represent a trusted name, but the domain name is generic and potentially suspicious. The lesson here is that employees need to ensure that the domain name matches the organization that they believe they are dealing with. An example of this is below.

Domain

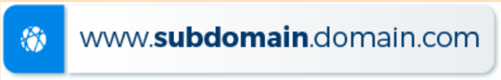
What is before .com/ .net/ .org/ .whatever



www.domain.com

Subdomain

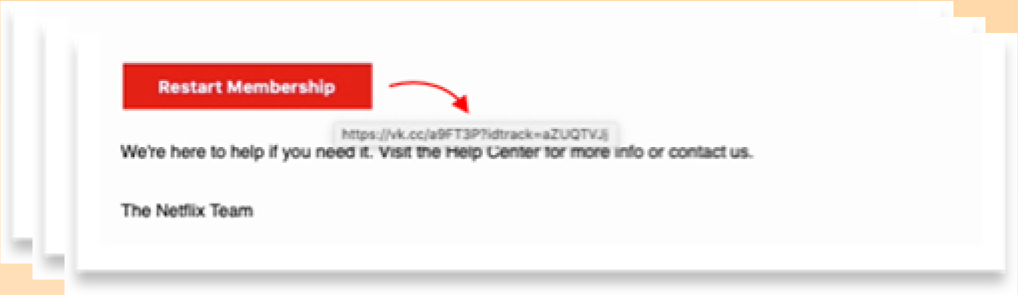
What is before your primary domain



www.**subdomain**.domain.com

"By Placing the Trusted Name in the 'Subdomain', Cyber Criminals can trick users into navigating to the Malicious 'Domain'"

2. The URL or any 'Action Button' in the email does not take a user to where they expect to go. Just as in the instance above, the URL has been manipulated, but in this case, the url is routing through an email sending service, and does not navigate directly to the trusted brand url. Users should HOVER over a url to ensure that a web address is in fact the same as the url that is advertised to them. See example here:

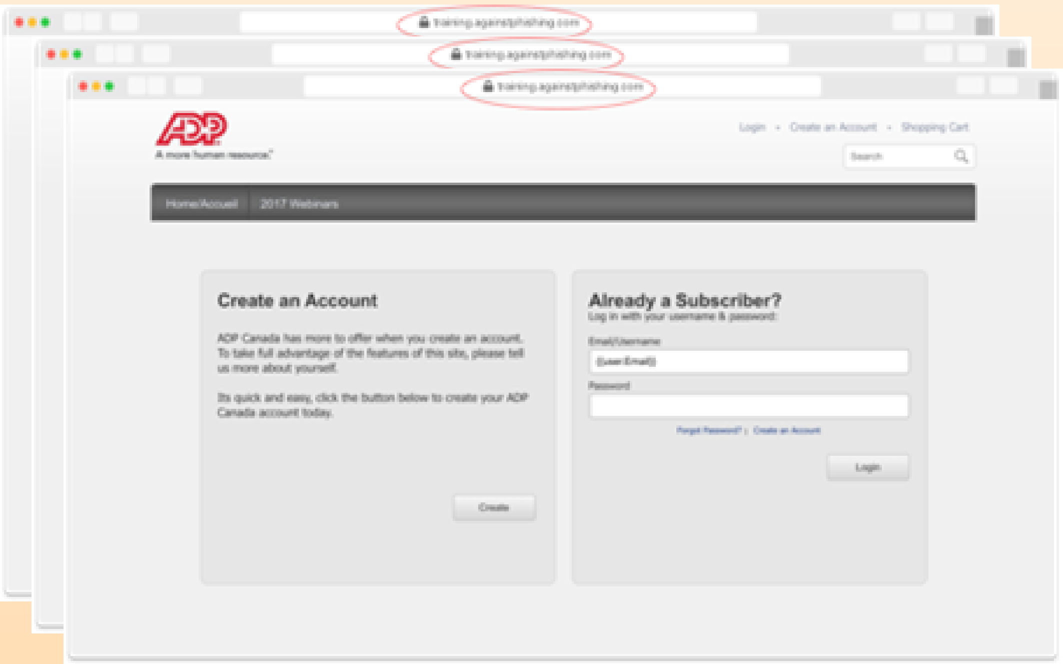


https://vk.cc/a9FT3P?idtrack=aZUQTVJj

We're here to help if you need it. Visit the Help Center for more info or contact us.

The Netflix Team

3. The destination landing page, if clicked on by the employee, will send them to a training landing page that will look like an authentic login page of the spoofed email, however, the url (web address) will clearly be different from the web address that the user would have expected to have navigated to. The lesson here is to always validate that the URL of the webpage is in fact where you expect to be (i.e., don't just pay attention to the logos and visuals). An example is below:


training.againstphishing.com
training.againstphishing.com
training.againstphishing.com
ADP
A more human resource.
Login • Create an Account • Shopping Cart
Search
Home/Accueil
2017 Webinars
Create
Email/Username
{{user.Email}}
Password
Forgot Password? | Create an Account
Login

Create an Account

ADP Canada has more to offer when you create an account. To take full advantage of the features of this site, please tell us more about yourself.

Its quick and easy, click the button below to create your ADP Canada account today.

Already a Subscriber?

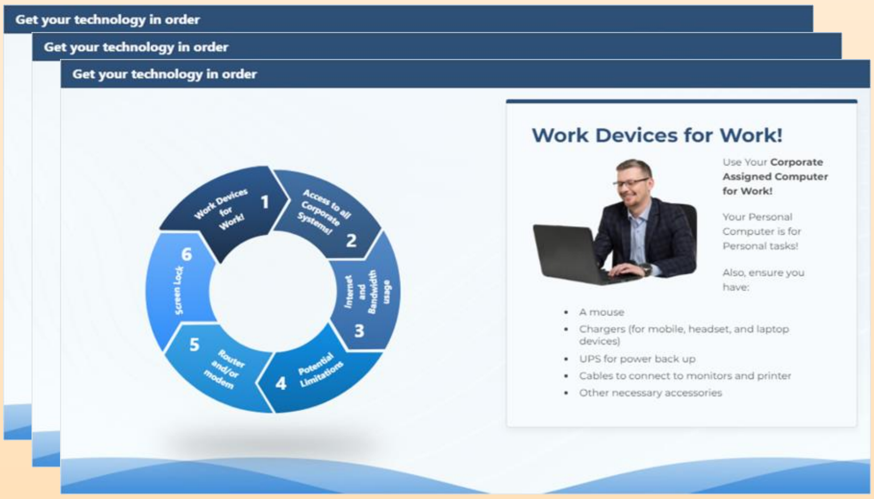
Log in with your username & password:

4. The final assessment and lesson is in the **ability to NOT engage with a potentially malicious website**. If the employee has not picked up on the first 3 opportunities to notice they are being phished, and they attempt to click within the 'Email/Username' or 'Password' fields above, or click on any of the 'Create' or 'Login' buttons above, those would trigger the pop up of a training document that would highlight to the user that they have been phished. In this case, the pop up indicates that this is a training exercise and that their data is safe.

Month 1:

- **Communication Launch**
- *(Optional)* Policy Review
- Dark Web Data Monitoring turned ON
- **Training Asset #1:** Identifying a Phishing Email
  - This video tactically assesses for users how to identify a phishing email with very specific learning lessons. Throughout the annual program, users will have many opportunities to demonstrate learning through successful phish email identification.

- **Training Asset #2**:
  Working from Home – Part 1
  - This video discusses the nature of remote working and the necessary tools such as CRMs and VPNs to achieve optimal virtual productivity and security.



Get your technology in order

Get your technology in order

Get your technology in order

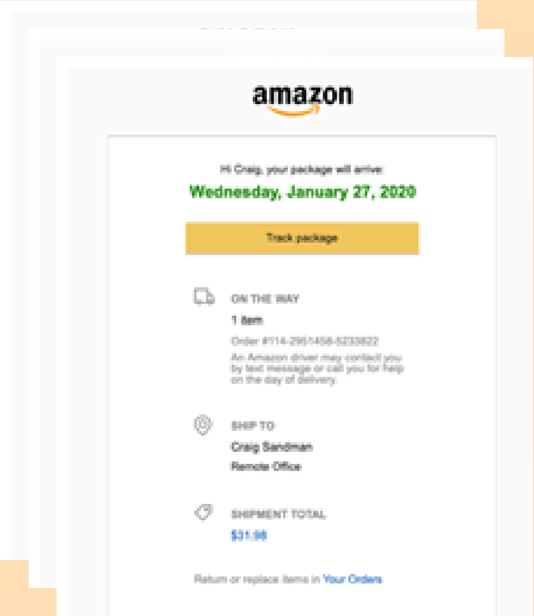
Work Devices for Work!

Use Your **Corporate Assigned Computer for Work!**

Your Personal Computer is for Personal tasks!

Also, ensure you have:

- A mouse
- Chargers (for mobile, headset, and laptop devices)
- UPS for power back up
- Cables to connect to monitors and printer
- Other necessary accessories



amazon

Hi Craig, your package will arrive:

Wednesday, January 27, 2020

Track package

ON THE WAY

1 item

Order #114-2951458-5233822

An Amazon driver may contact you by text message or call you for help on the day of delivery.

SHIP TO

Craig Sandman

Remote Office

SHIPMENT TOTAL

$31.98

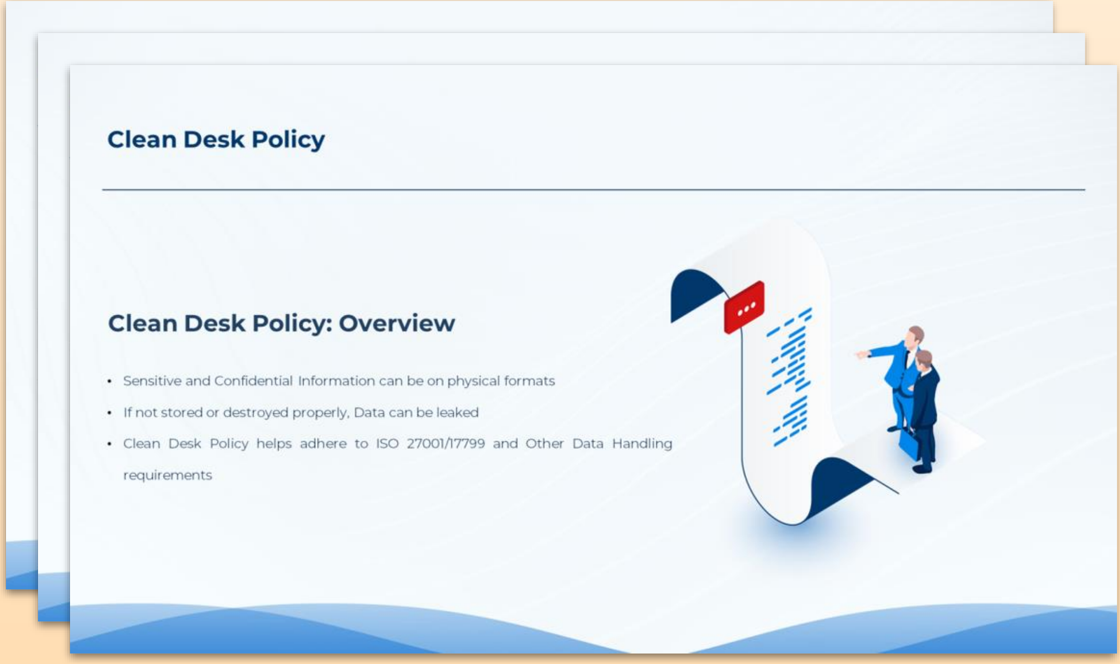
Return or replace items in Your Orders

- **Phishing Simulation:** Amazon Package Delivery (preview image)
  - Basic Brand Spoof Phishing Email that immediately challenges users to validate email Sender and Domain information vs. relying on the visuals of email.

Month 2:

- **Reporting from Prior Month** sent for review and assessment
- **Dark Web Data Monitoring** activities ongoing

- **Training Asset #3:** Clean Desk Policy
    - This video provides an overview of a clean desk policy and reasons why it is important to maintain a clean desk for cyber safety.



Clean Desk Policy

Clean Desk Policy: Overview

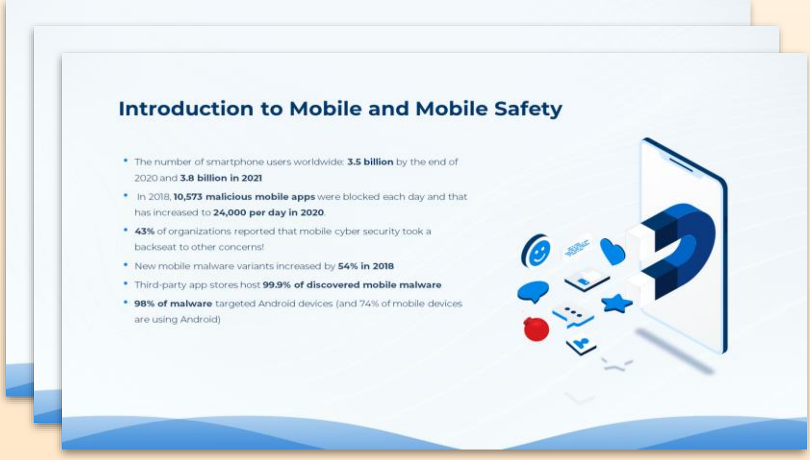
- Sensitive and Confidential Information can be on physical formats
- If not stored or destroyed properly, Data can be leaked
- Clean Desk Policy helps adhere to ISO 27001/17799 and Other Data Handling requirements

- **Phishing Simulation: Microsoft** - Security Update
    - Microsoft - Security update Template is designed for users to click on the link regarding Virus threats for Microsoft outlook. The Landing page will prompt the user to sign in by an email address. Users should notice that: sender name is not from 'Microsoft', hovering over links do not point to 'Microsoft' and landing page is not the Microsoft URL
- **Phishing Simulation: Slack**- (Important Security Notice)
    - Slack (important Security Notice) is Designed to inform users there has been unauthorized access to the Slack Database and 2FA (Two Factor Authentication) is available to set up by clicking one of the available links in the notice. The Slack Landing Page will prompt for an email address and password. Users should notice that: sender name is not from 'Slack', hovering over links do not point to 'Slack' and landing page is not the Slack URL.

Month 3:

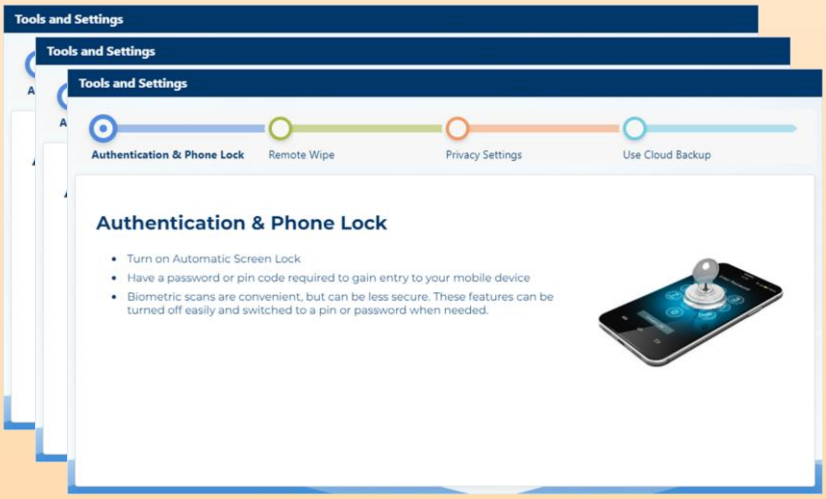
- **Reporting from Prior Month** sent for review and assessment
- **Dark Web Data Monitoring** activities ongoing

- **Training Asset #4:** Mobile Security - Part 1
  - This video introduces the topic of mobile malware and keeping your mobile devices safe from phishing attacks.



Introduction to Mobile and Mobile Safety

- The number of smartphone users worldwide: **3.5 billion** by the end of 2020 and **3.8 billion in 2021**
- In 2018, **10,573 malicious mobile apps** were blocked each day and that has increased to **24,000 per day in 2020**.
- **43%** of organizations reported that mobile cyber security took a backseat to other concerns!
- New mobile malware variants increased by **54% in 2018**
- Third-party app stores host **99.9% of discovered mobile malware**
- **98% of malware** targeted Android devices (and 74% of mobile devices are using Android)



Tools and Settings

Authentication & Phone Lock

- Turn on Automatic Screen Lock
- Have a password or pin code required to gain entry to your mobile device
- Biometric scans are convenient, but can be less secure. These features can be turned off easily and switched to a pin or password when needed.

- **Training Asset #5:** Mobile Security - Part 2
  - This video builds upon the topic of mobile security, focusing on the ideal methods to keep your personal information private and secure on your mobile device.

- **Phishing Simulation**: **LinkedIn - Verification Required**
  - LinkedIn - Verification Required Template is designed for users to update their LinkedIn account by login in. The landing page will prompt the user for an email address and password. Users should notice that: Sender name is not from 'LinkedIn', hovering over Links and 'Update' button do not point to 'LinkedIn' and landing page is not the LinkedIn URL
- **Phishing Simulation**: **Microsoft Password Reset**
  - Microsoft Password Reset Template is designed for users to sign in to reset their password by clicking on the link. The landing Page will prompt the user to enter an email address. Users should notice that: sender name is not from 'Microsoft', hovering over links do not point to 'Microsoft' and landing page is not the Microsoft URL

Month 4:

- **Reporting from Prior Month** sent for review and assessment
- **Dark Web Data Monitoring** activities ongoing

- **Training Asset #6**: Social Media Phishing - Part 1
    - This video focuses on the basics of social media phishing.

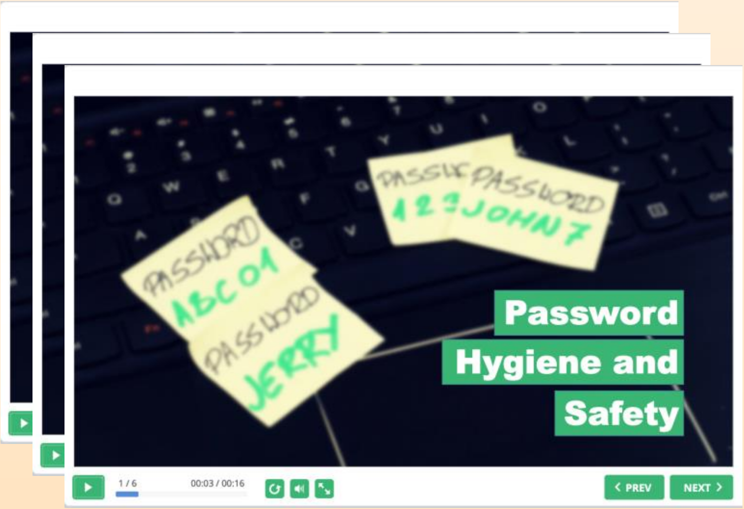
How are criminals leveraging Social Media
How are criminals leveraging Social Media
How are criminals leveraging Social Media
1
2
3
4
5
Creating Fake Identities to conduct Cyber Crimes

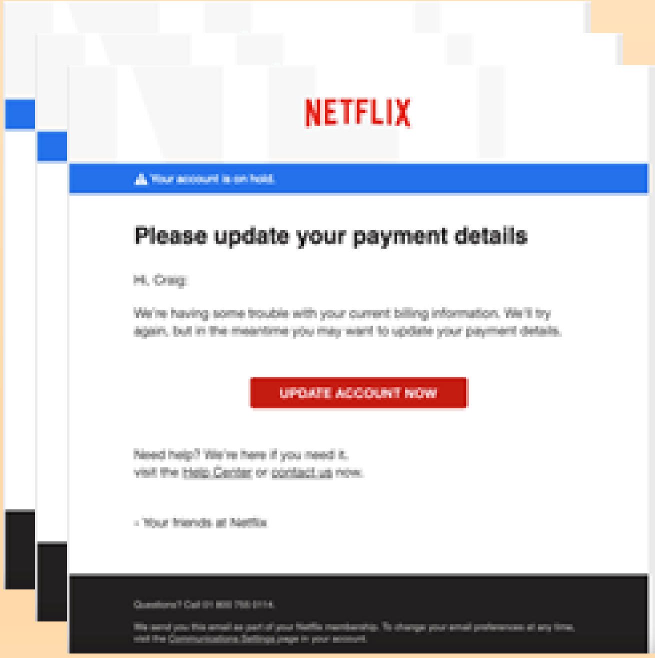
- **Phishing Simulation**: **Google Sheets** (Document Invitation)
    - Google Sheets (Document Invitation) Template is designed for users to open a Google Sheet via invite. The "Open in Sheets" button will send the user to the landing page and will prompt the user for an email address and password. Users should notice that: Sender name is not from 'Google', hovering over 'Open in Sheets' button does not point to 'Google' and landing page is not the Google URL.
- **Phishing Simulation**: **Zoom Meeting Invitation**
    - Zoom Meeting template is designed for users to sign in to their Zoom account for a scheduled meeting by Clicking the "share-zoom" link. By clicking the link it will direct users to the Zoom landing page and prompt for an username and password. Users should recognize that: sender name is not from 'Zoom', links do not point to 'Zoom' and landing page is not the Zoom URL.

Month 5:

- **Reporting from Prior Month** sent for review and assessment
- **Dark Web Data Monitoring** activities ongoing

- **Training Asset #8**: Password Hygiene and Safety
    - Compromised passwords are present in 67% of data breaches. Properly securing your access with Strong, Complex, and Unique passwords can significantly lower your risk. Learn more in this training!





NETFLIX

Your account is on hold.

Please update your payment details

Hi, Craig:

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

Need help? We're here if you need it.
visit the Help Center or contact us now.

- Your friends at Netflix

Questions? Call 01 800 750 0114.

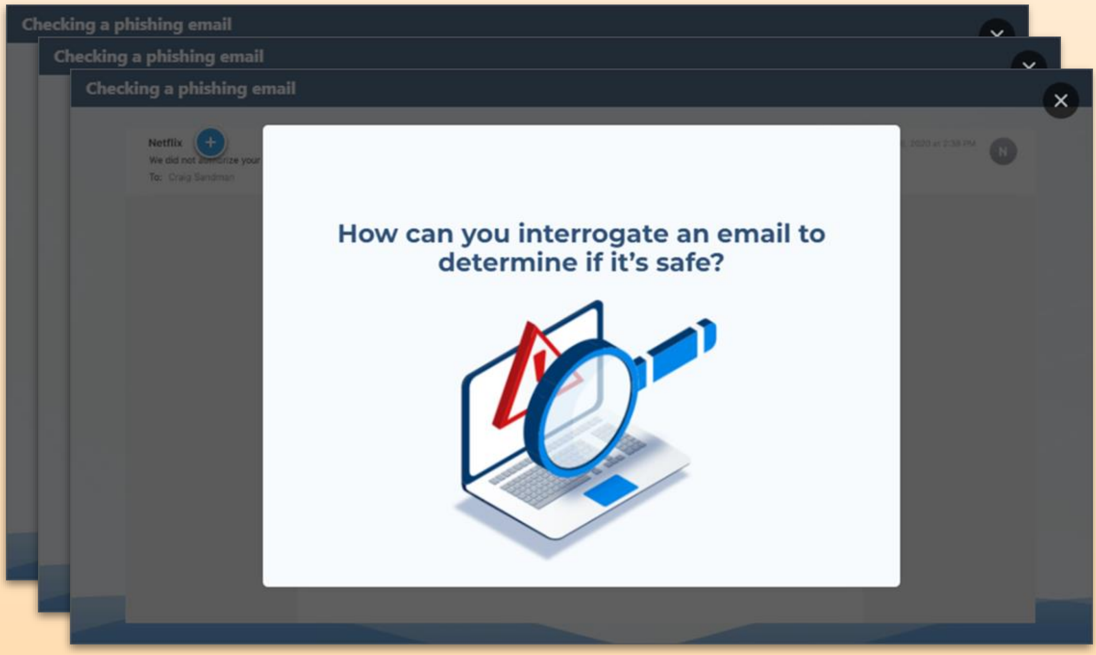
We send you this email as part of your Netflix membership. To change your email preferences at any time, visit the Communications Settings page in your account.

- **Phishing Simulation**: Netflix (Restore Password)
    - Netflix (Restore Password) Template is designed for users login to reset their account password by clicking on the "Restore Password" button . The landing page will prompt the user for an email address and password. Users should notice that: sender name is not from 'Netflix', hovering over links and 'Restore Password' button do not point to 'Netflix' and landing page is not the Netflix URL

Month 6:

- **Reporting from Prior Month** sent for review and assessment
- **Dark Web Data Monitoring** activities ongoing

- **Training Asset #9:** Working From Home - Part 2
  - This video is a review of the dangers of avoiding phishing attacks and scams while working from home. The asset also discusses avoiding 'vishing' or Voice Phishing Scams as well.


Checking a phishing email
Checking a phishing email
Checking a phishing email
Netflix
To: Craig Sandman

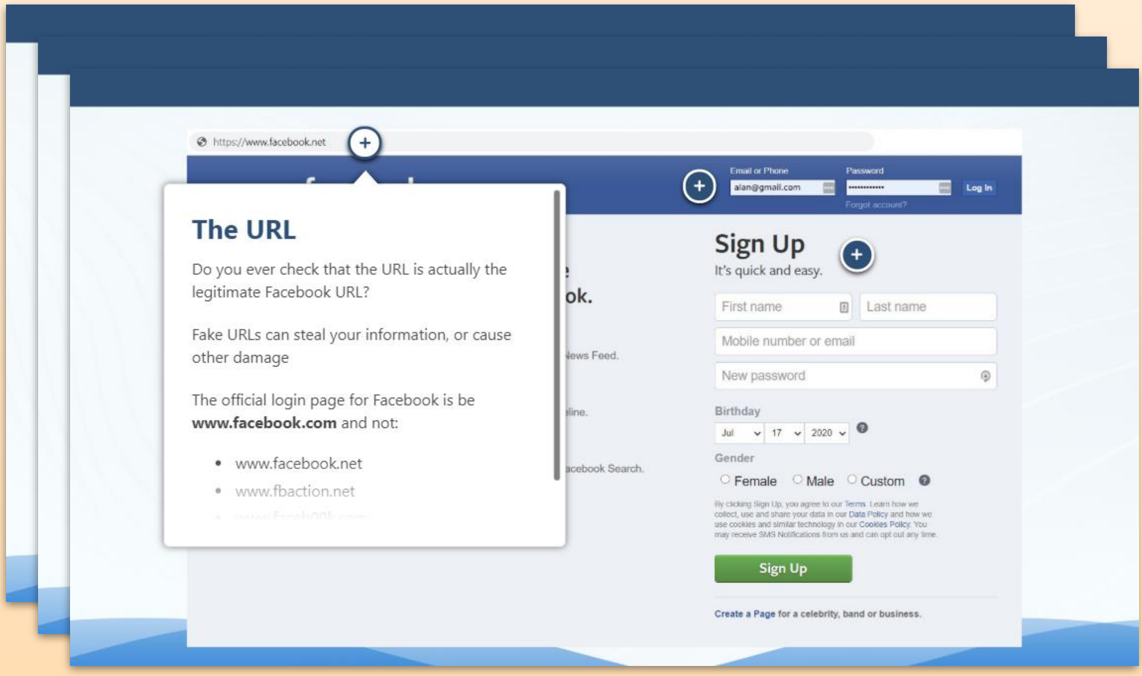
How can you interrogate an email to determine if it's safe?

- **Phishing Simulation: Dropbox** - Shared Folder
  - Dropbox - Shared Folder Template is designed for users to sign in to open a shared folder. By clicking the "Go to folder" Button it will direct users to a landing page and prompt the user to enter an email and Password. Users should notice that: sender name is not from 'Dropbox', hovering over Links and 'Go to folder' button do not point to 'Dropbox' and landing page is not the Dropbox URL.
- **Phishing Simulation: FedEx** (Tracking, Shipping and Locations)
  - FedEx (Tracking,Shipping and Locations) Template is designed for users to open their account due to an undelivered package. By Clicking on the landing page it will prompt the user to sign into their FedEx account. Users should notice that: sender name is not from 'FedEx', hovering over Links do not point to 'FedEx' and landing page is not the FedEx URL.

Month 7:

- **Reporting from Prior Month** sent for review and assessment
- **Dark Web Data Monitoring** activities ongoing

- **Training Asset #10:** Social Media Phishing - Part 2
  - This video focuses on social media phishing, specifically cybersecurity attacks and scams centered around FaceBook users.



The URL

Do you ever check that the URL is actually the legitimate Facebook URL?

Fake URLs can steal your information, or cause other damage

The official login page for Facebook is be **www.facebook.com** and not:

- www.facebook.net
- www.fbaction.net

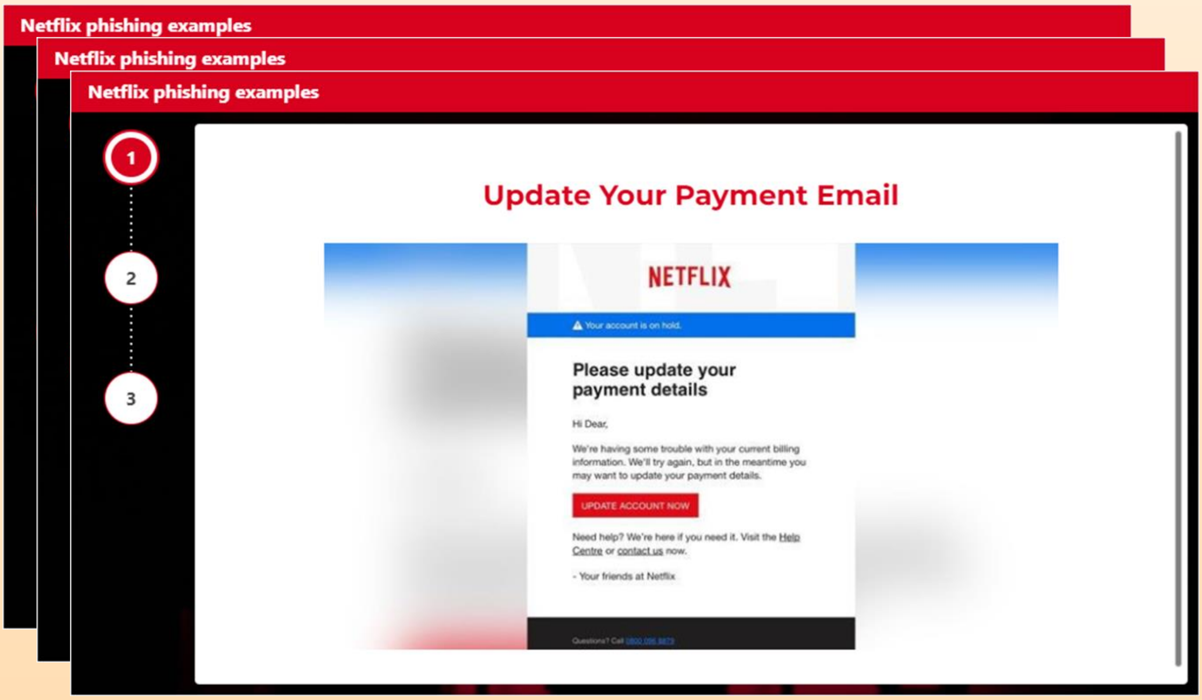
By clicking Sign Up, you agree to our Terms. Learn how we collect, use and share your data in our Data Policy and how we use cookies and similar technology in our Cookies Policy. You may receive SMS Notifications from us and can opt out any time.

- **Phishing Simulation: Office 365** - Undelivered Messages
  - Office 365 - Undelivered Messages Template is designed for users to let them know that messages have not been delivered and they can fix it by clicking the "Send Again" button. The Office 365 landing page will prompt users for an email and password. Users should notice that: sender name is not from 'Microsoft', hovering over links and 'Send Again' button do not point to 'Microsoft' and landing page is not the Microsoft URL.
- **Phishing Simulation: SharePoint Project Creation**
  - SharePoint Project Creation Template is designed to inform users their Project MailBox has been created for their account and they can sign in by clicking the "Go to the site" link. The landing page will prompt for an email address and password. Users should notice that: sender name is not from 'SharePoint', hovering over links do not point to 'Sharepoint' and landing page is not the Sharepoint URL.

Month 8:

- **Reporting from Prior Month** sent for review and assessment
- **Dark Web Data Monitoring** activities ongoing

- **Training Asset #11:** Netflix Scams
  - This video focuses on scams and phishing attempts surrounding Netflix.



Netflix phishing examples

Netflix phishing examples

Netflix phishing examples

Update Your Payment Email

Your account is on hold.

Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

Need help? We're here if you need it. Visit the Help Centre or contact us now.

- Your friends at Netflix

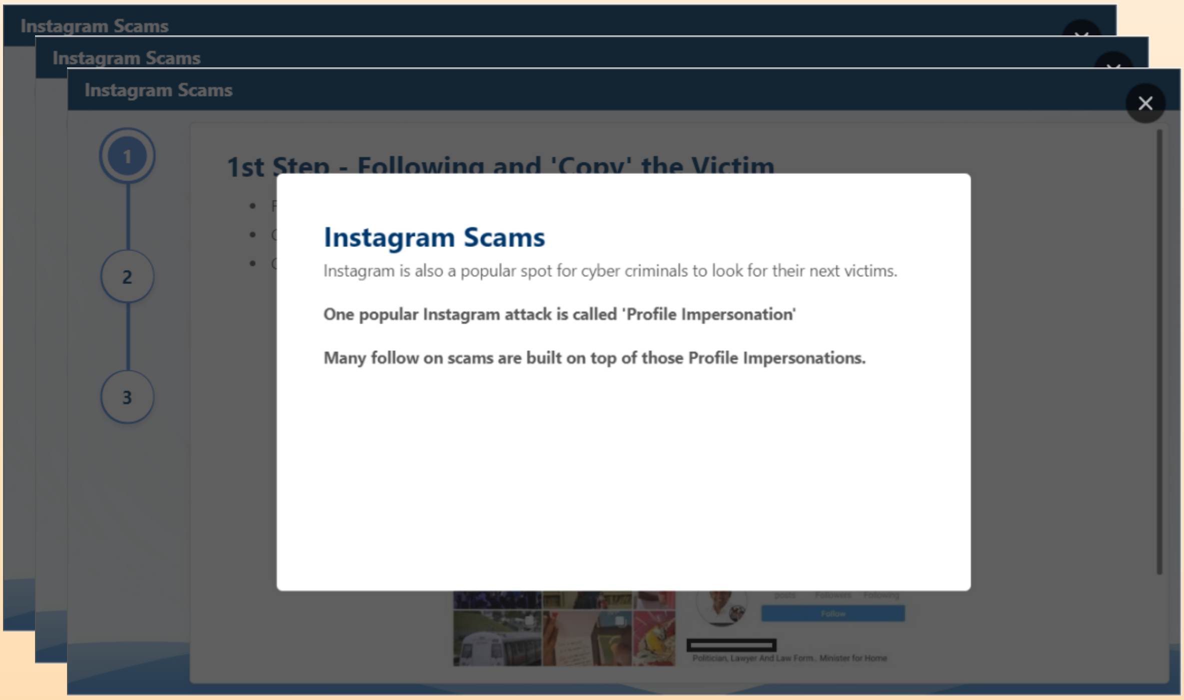
Questions? Call [illegible]

- **Phishing Simulation: Office 365** (Change Password)
  - Office 365 - Change Password Template is designed for users to sign in to change their account password by clicking on the "click here" link. The Office 365 landing page will prompt users for an account password. Users should notice that: sender name is not from 'Microsoft', hovering over links do not point to 'Microsoft' and landing page is not the Microsoft URL.
- **Phishing Simulation: Yahoo** - Mobile Number Removed
  - Yahoo - Mobile Number Removed Template is designed to inform users a mobile number has been removed from their account. If the user did not make this change they can sign in to their account by Clicking the blue login link that will direct users to the Yahoo landing page that will prompt for an email address. Users should recognize that: sender name is not from 'Yahoo', links do not point to 'Yahoo' and landing page is not the Yahoo URL.

Month 9:

- **Reporting from Prior Month** sent for review and assessment
- **Dark Web Data Monitoring** activities ongoing

- **Training Asset #12**: Social Media Phishing - Part 3
  - This video focuses on phishing attacks, specifically targeting Instagram users.



Instagram Scams

Instagram is also a popular spot for cyber criminals to look for their next victims.

One popular Instagram attack is called 'Profile Impersonation'

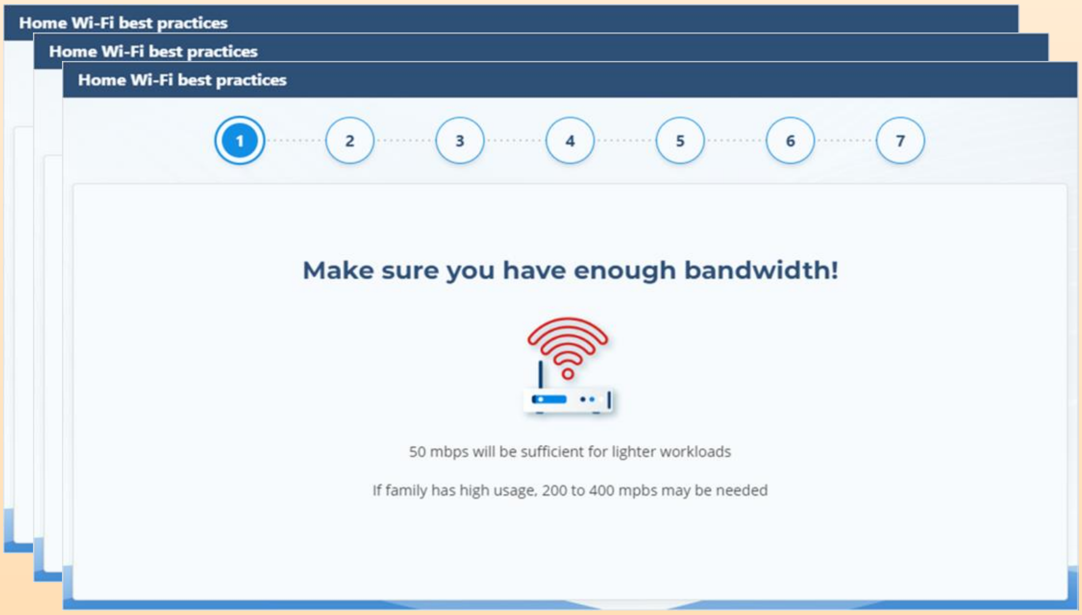
Many follow on scams are built on top of those Profile Impersonations.

- **Phishing Simulation: Instagram** - Verify Your Account
  - Instagram Verify Your Account Template is designed for users to login to their account due to an suspicious attempted login. The landing page will prompt the user for an email address or name. Users should notice that: sender name is not from 'Instagram', hovering over links do not point to 'Instagram' and landing page is not the Instagram URL.

Month 10:

- **Reporting from Prior Month** sent for review and assessment
- **Dark Web Data Monitoring** activities ongoing

- **Training Asset #13**: Working From Home - Part 3
  - This video discusses keys to remote working security such as Safe Wifi and Wifi Password Management.



Home Wi-Fi best practices

Home Wi-Fi best practices

Home Wi-Fi best practices

Make sure you have enough bandwidth!

50 mbps will be sufficient for lighter workloads

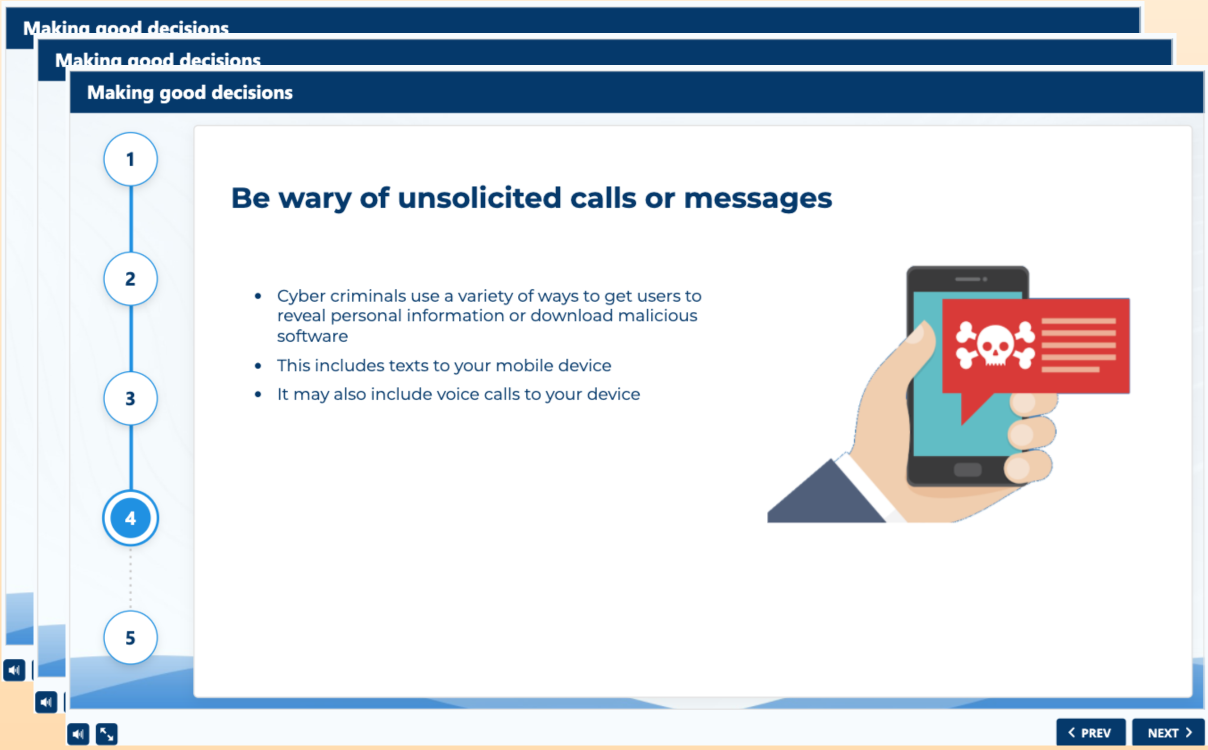
If family has high usage, 200 to 400 mpbs may be needed

- **Phishing Simulation: Microsoft** - Unusual Sign-in
  - Microsoft - Unusual Sign-in Template is designed to get users to click on the "review recent activity" button due to there being a sign in attempt on their account. The landing Page will prompt a user for an email address. Users should notice that: sender name is not from 'Microsoft', hovering over links and buttons do not point to 'Microsoft' and landing page is not the Microsoft URL.
- **Phishing Simulation: Google** - Access Granted
  - Google Access Granted Template is designed for users to check activity on their google account by clicking the "Check activity" button. The "Check activity" button will send the user to sign in to the landing page and will prompt for an email address and password for their google account. Users should notice that: sender name is not from 'Google', hovering over 'Check Activity' button does not point to 'Google' and landing page is not the Google URL.

Month 11:

- **Reporting from Prior Month** sent for review and assessment
- **Dark Web Data Monitoring** activities ongoing

- **Training Asset #13:** Mobile Security - Part 3
  - This video focuses on safe wifi systems and the risk of private information on apps or websites being used for phishing attacks.



Making good decisions

Making good decisions

Making good decisions

Be wary of unsolicited calls or messages

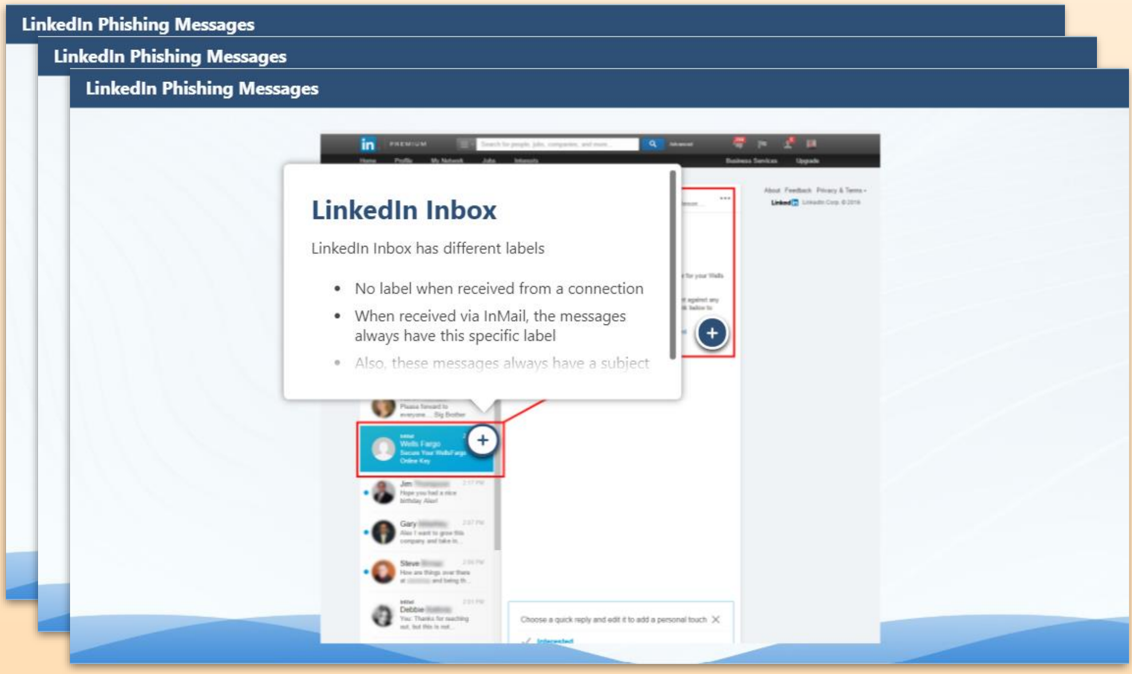
- Cyber criminals use a variety of ways to get users to reveal personal information or download malicious software
- This includes texts to your mobile device
- It may also include voice calls to your device

- **Phishing Simulation: PayPal** - Confirm Phone Number
  - PayPal - Confirm Phone Number Template is designed for users to click the “confirm Phone: button and sign in to confirm a phone number associated with the PayPal account. The landing page will prompt for an email address. Users should notice that: Sender name is not from ‘Paypal’, hovering over links and 'Confirm Phone' button do not point to ‘PayPal’ and landing page is not the PayPal URL.

Month 12:

- **Reporting from Prior Month** sent for review and assessment
- **Dark Web Data Monitoring** activities ongoing

- **Training Asset #14:** Social Media Phishing - Part 4
    - This video focuses on phishing attacks, targeted at Linkedin users.



LinkedIn Phishing Messages

LinkedIn Phishing Messages

LinkedIn Phishing Messages

LinkedIn Inbox

LinkedIn Inbox has different labels

- No label when received from a connection
- When received via InMail, the messages always have this specific label
- Also, these messages always have a subject

- **Phishing Simulation: Internal Message** - Windows 10 Upgrade Error
    - Internal Message - Windows 10 Upgrade Error Template is designed for users to click the “Windows 10 Upgrade Support Site” link and sign in to resolve errors from an attempted update. The landing page will prompt for an email address and password. Users should notice that: sender name is not from ‘Microsoft’, hovering over links do not point to ‘Microsoft’ and landing page is not the Microsoft URL

Get in touch with Digital Beachhead for more details

www.digitalbeachhead.com

+1 (866) 879-1226

info@digitalbeachhead.com

company/digital-beachhead-inc