



**proofpoint®**



**CHANGE  
CHAMPIONS**

# **BC Security Day 2019**

November 2019

# Agenda

- **Proofpoint/Change Champions – Who Are We?**
- **Latest Global Threat Landscape Overview**
- **Mr. Potato Head!!!**
- **What Do They Want From Me?**
- **Recommendations To Stay Safe**



# proofpoint. Overview

The leader in protecting people from advanced threats and compliance risk

The most trusted  
partner to protect the  
leading threat vector

#1

Most deployed solution  
for the Fortune 100

#1

Most deployed solution  
for the Fortune 1000

#1

Most deployed solution  
for the Global 2000



Gartner Leader  
Sim & Training

Unparalleled visibility  
into Phishing Threats



128 of 144  
Global ISP's

Consumer  
Email visibility

Seamless integration  
with other next gen  
leaders



splunk>



okta

# Security Awareness Programs



## Award-winning programs

Our cybersecurity awareness programs have received awards and are used by some of Canada's and the world's leading organizations.



## Experts in change.

We are a team of change managers, communication experts, organizational psychologists, and trainers with a particular interest in IT security. Behavioral change is where we live.



## Customization that works

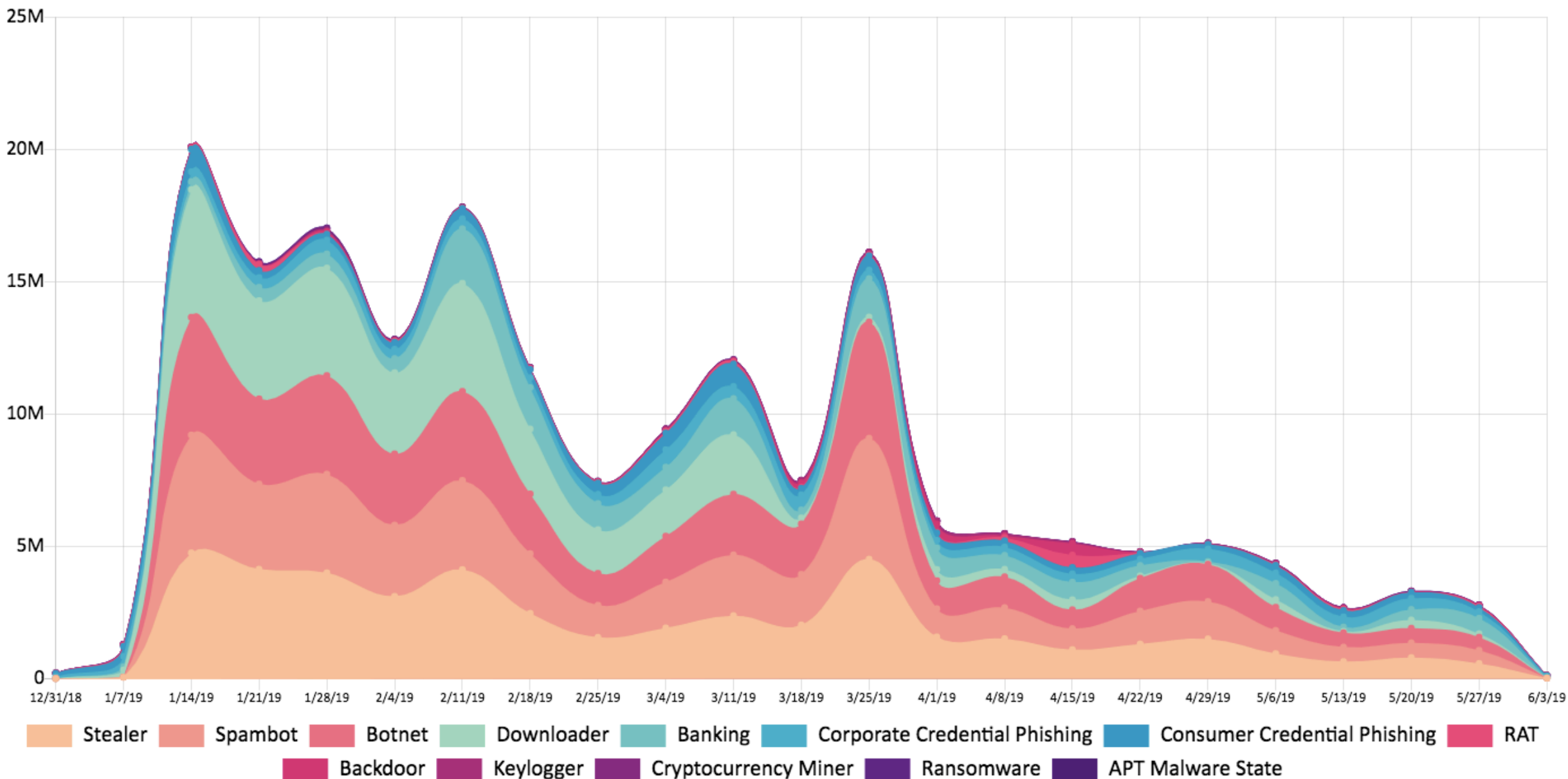
We know that each client is unique, which is why we tailor our program to meet the different needs of your organization.



## Proven approach and cost-effective option.

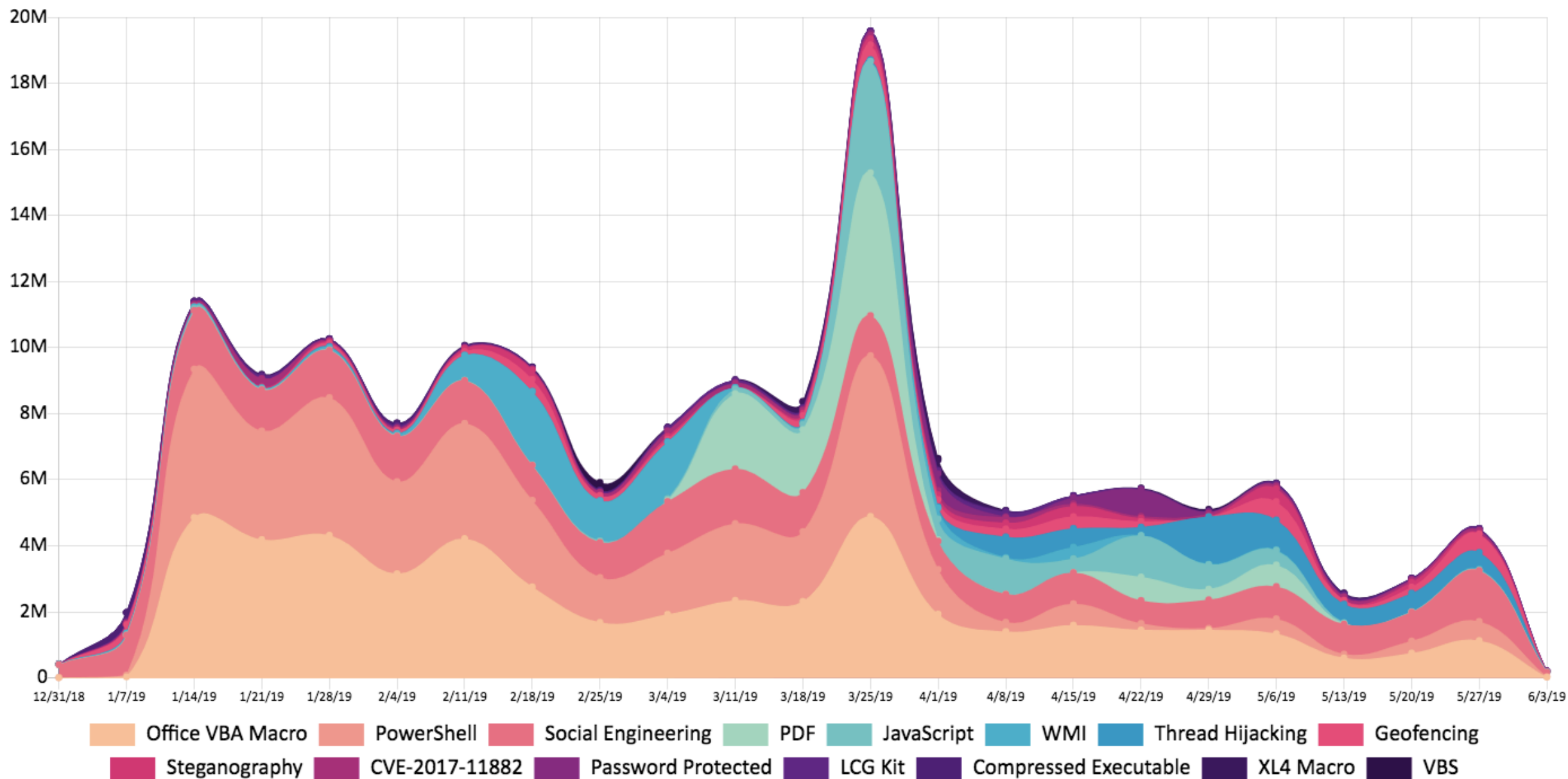
Our repeatable approach and experience allow us to onboard fast and have your program off the ground in a matter of weeks and with less than one FTE of effort.

# Global Threat Trends





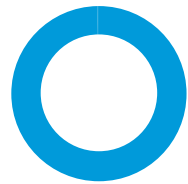
# Email Threat Landscape by Exploit Type





# Attacks increasingly target people, not infrastructure

## THREATS USE SOCIAL ENGINEERING, NOT VULNERABILITIES



**99%+**

Malware attacks rely on user to run malicious code



**300%+**

Increase in corporate credential phishing

Source: Proofpoint Threat Data.

## SHIFT TO CLOUD CREATES NEW THREAT VECTORS, DATA EXPOSURE



Account takeover of cloud apps is a growing problem

**63%**

Orgs exposed to targeted attacks

**37%**

Orgs detected successful breach

Source: Proofpoint Threat Data.

## EMAIL FRAUD IS A BOARD-LEVEL ISSUE



**\$12.5B+**

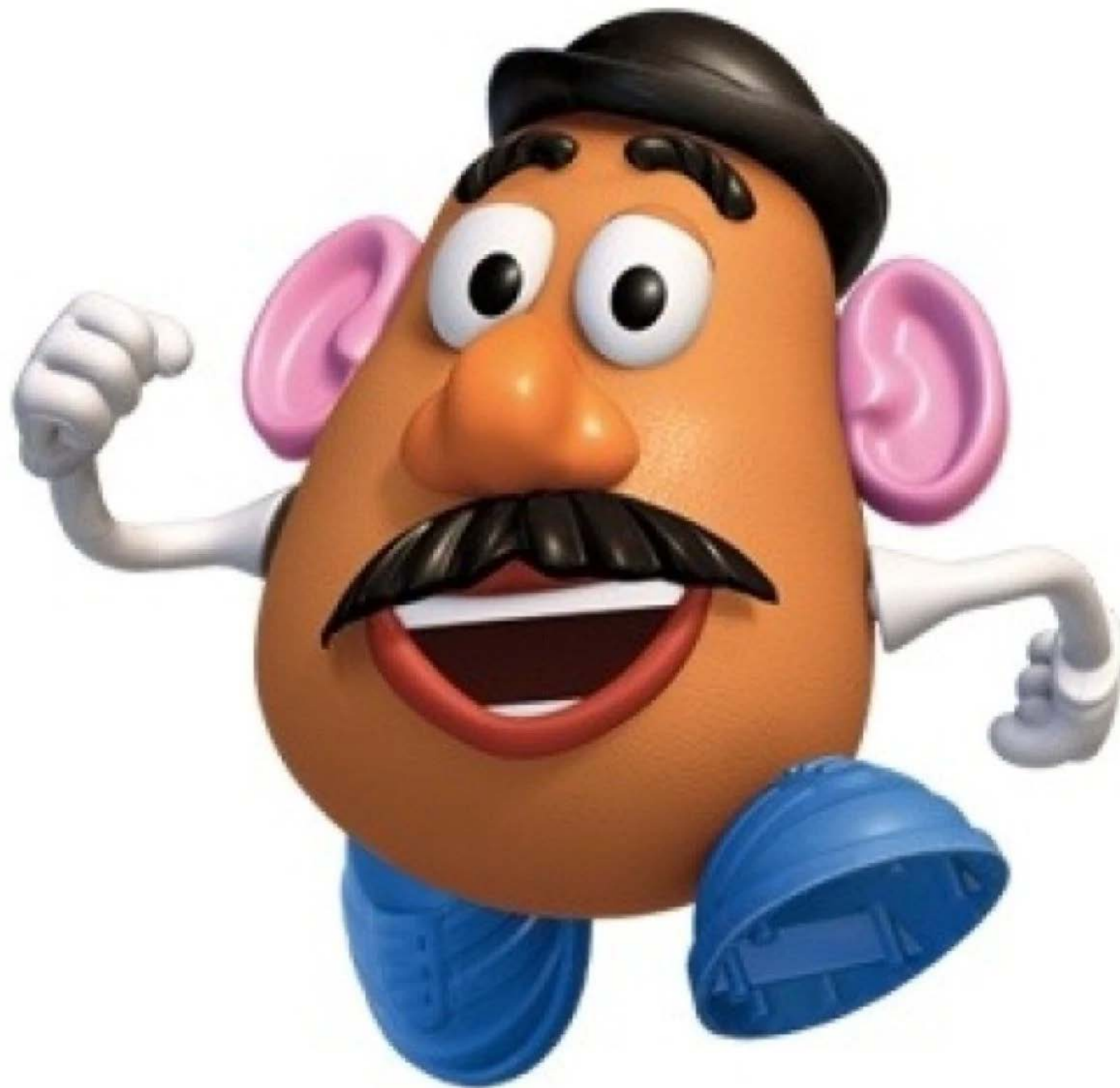
Direct losses worldwide  
(Oct 2013–May 2018)

**78,617**

Incidents worldwide

Source: FBI.

# Attack Structures....





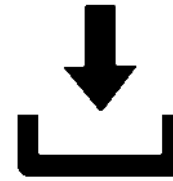
Script



Attachment



Exploit



File Download



Email



Link



Malicious Website



Stolen Credentials



Malware



Email



Link



Malicious Website



Stolen Credentials



Malware



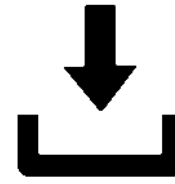
Attachment



Script

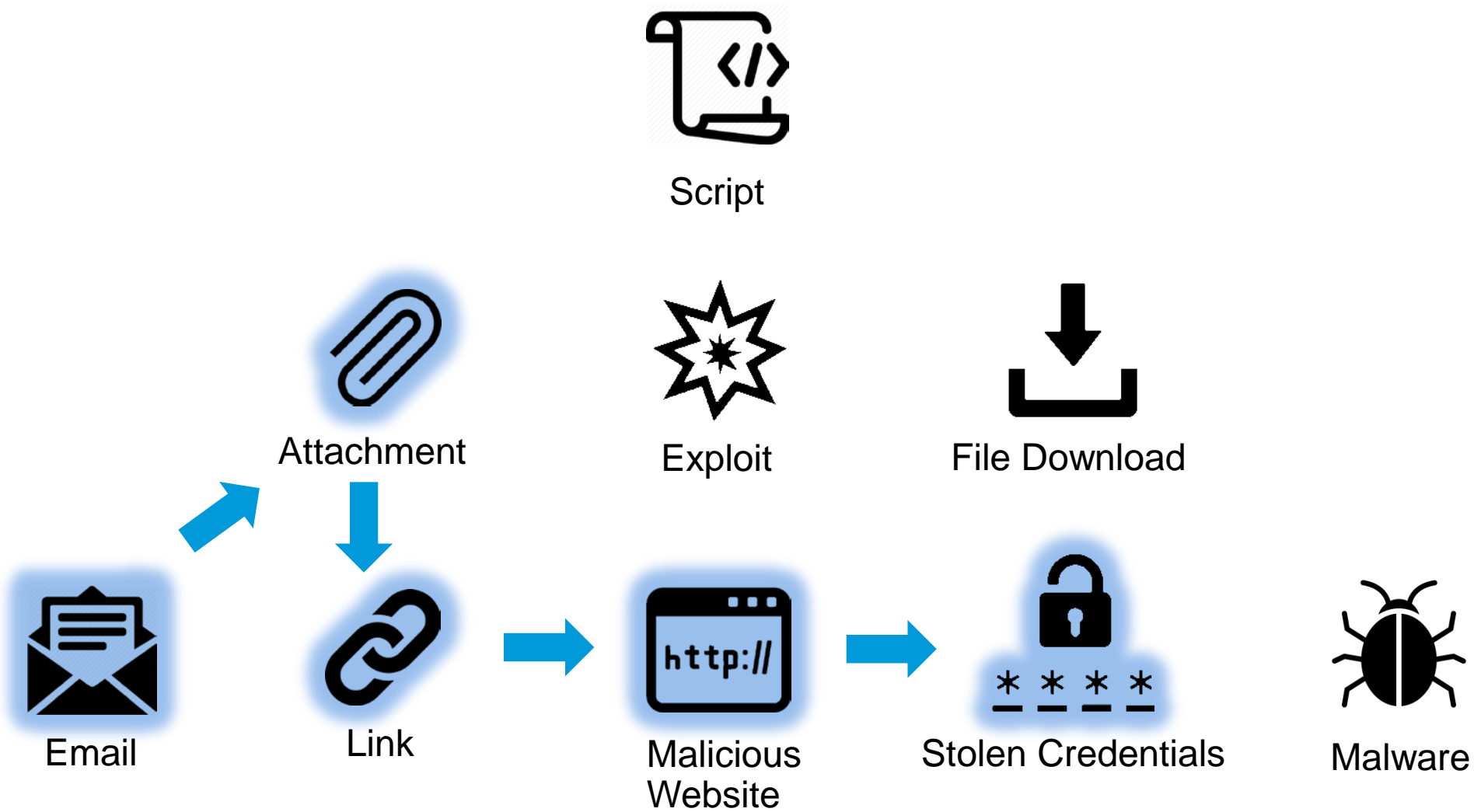


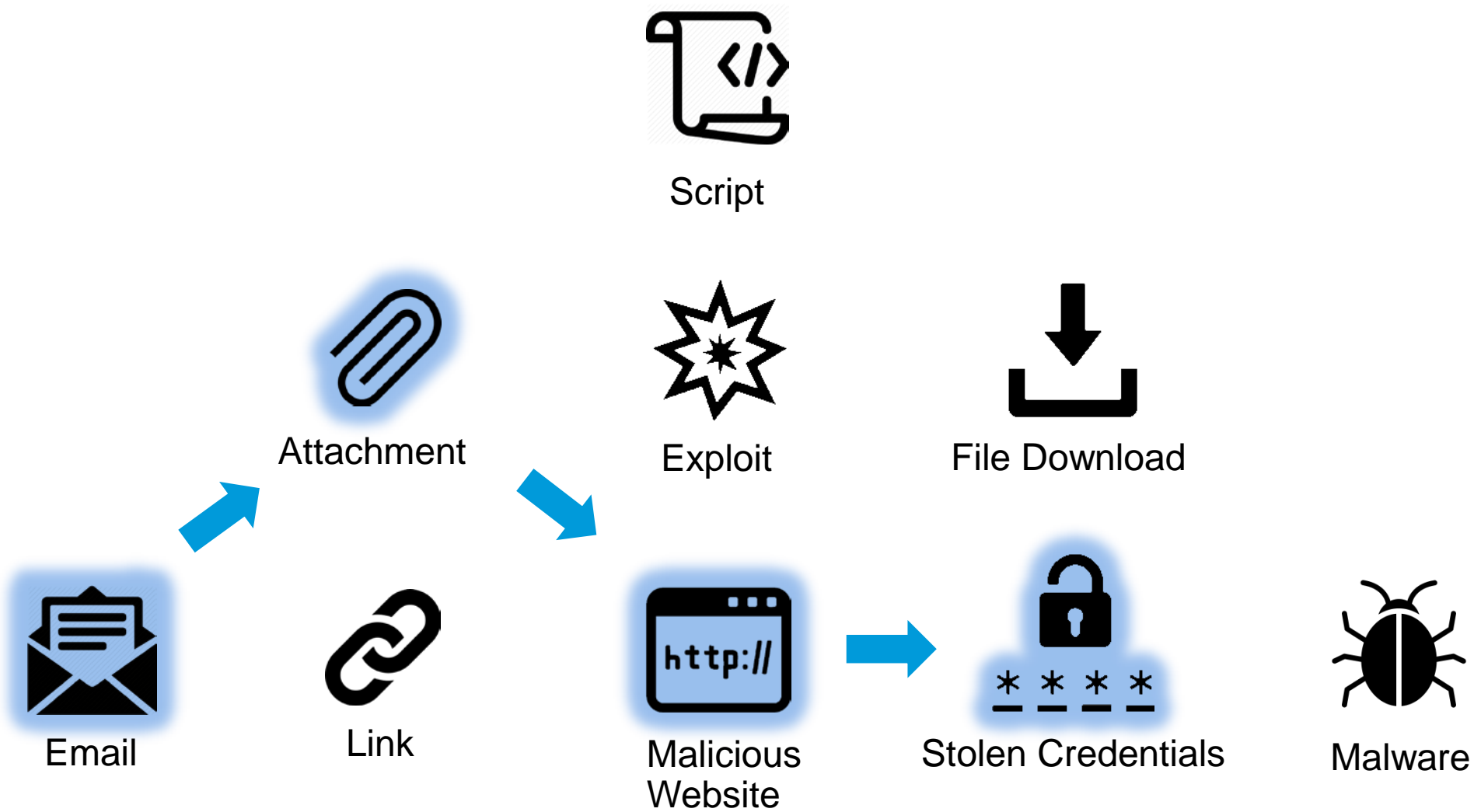
Exploit

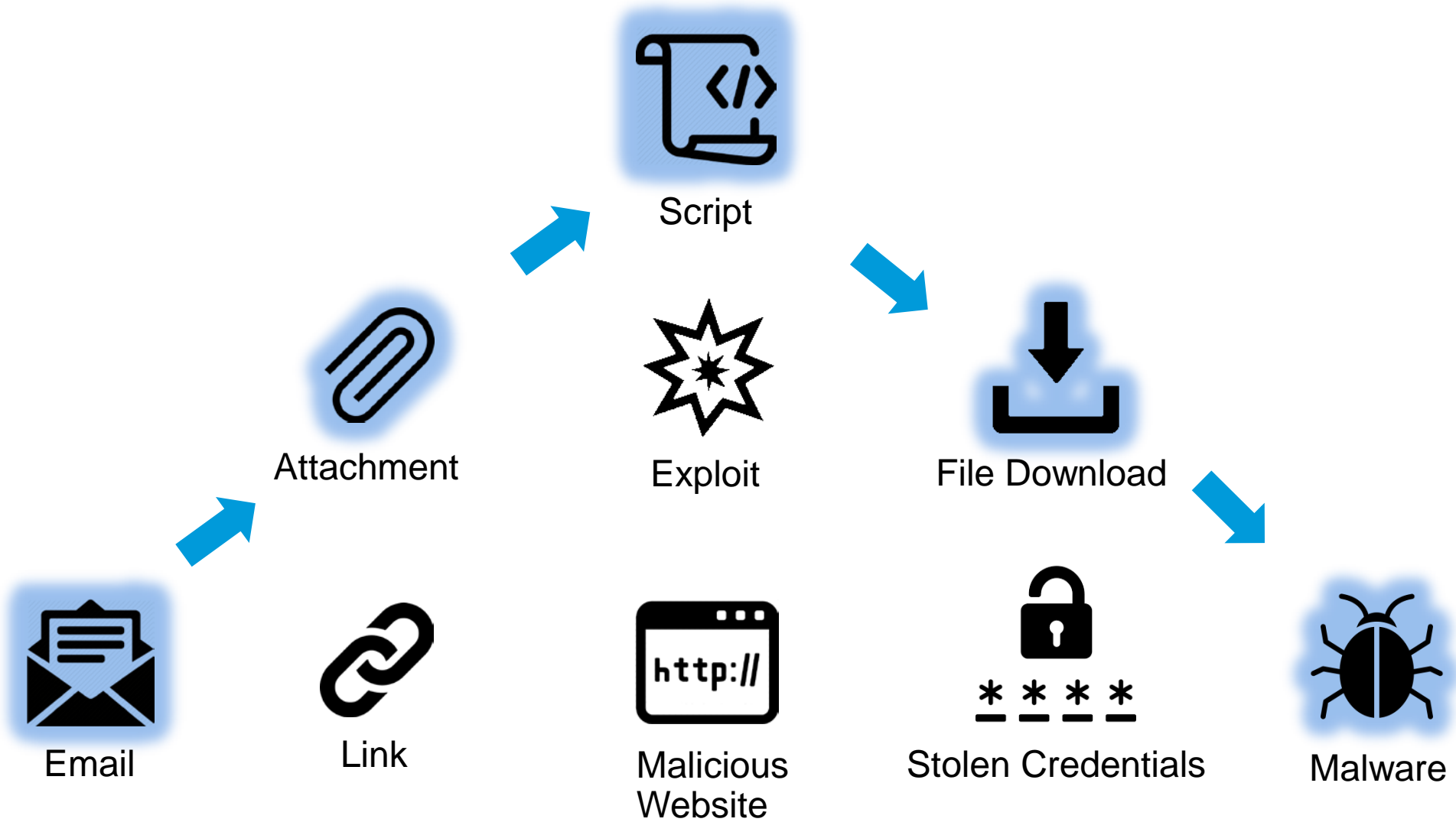


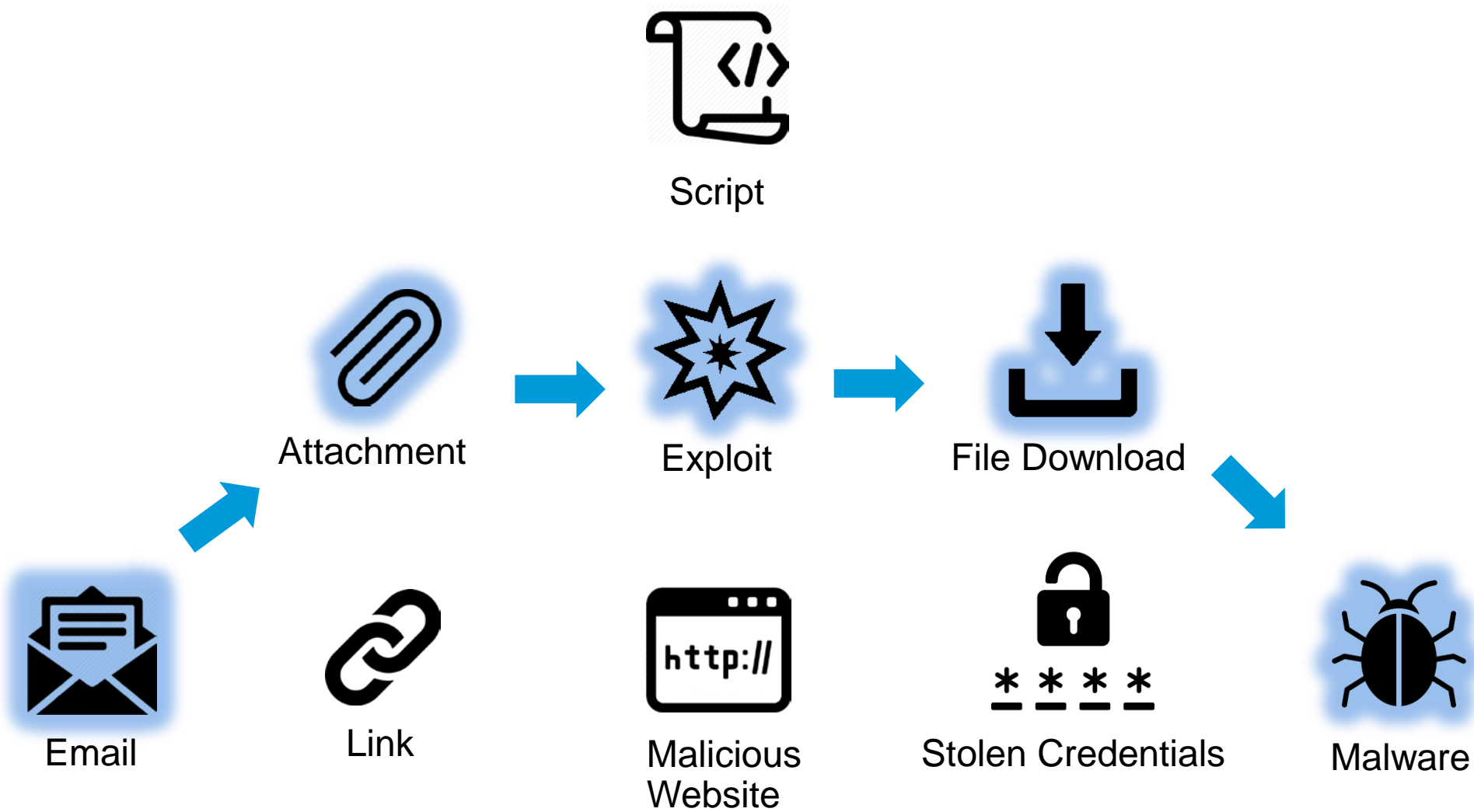
File Download

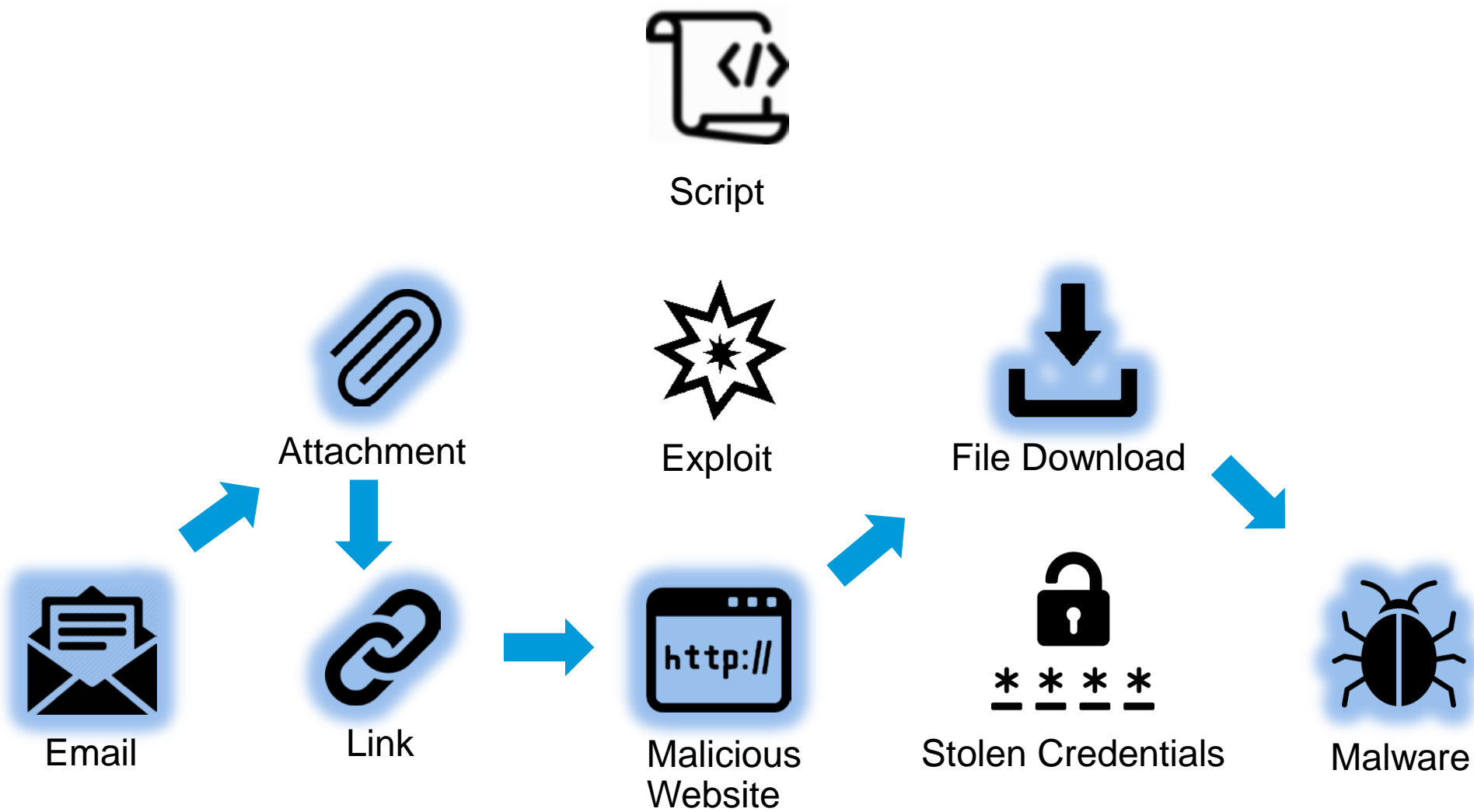




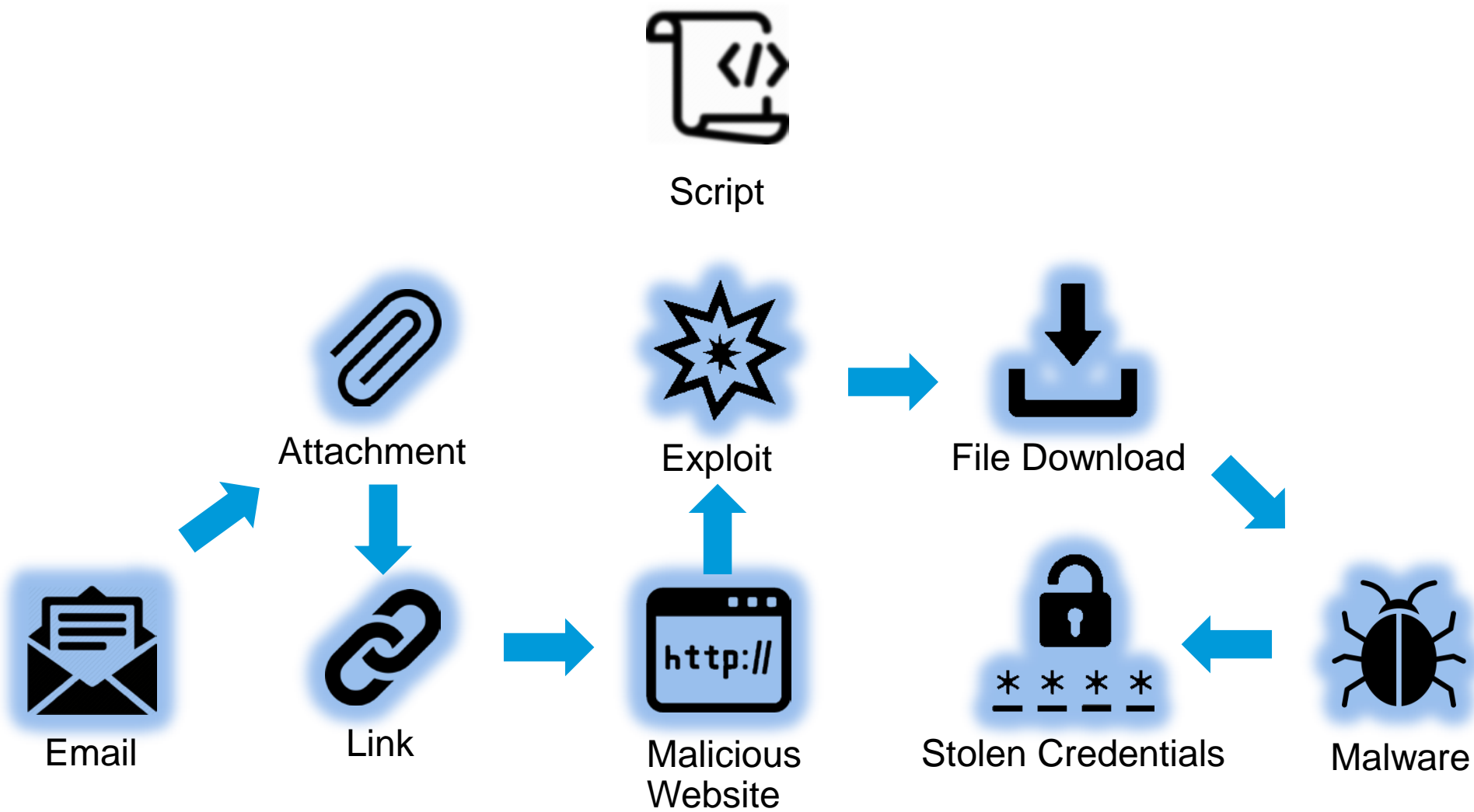


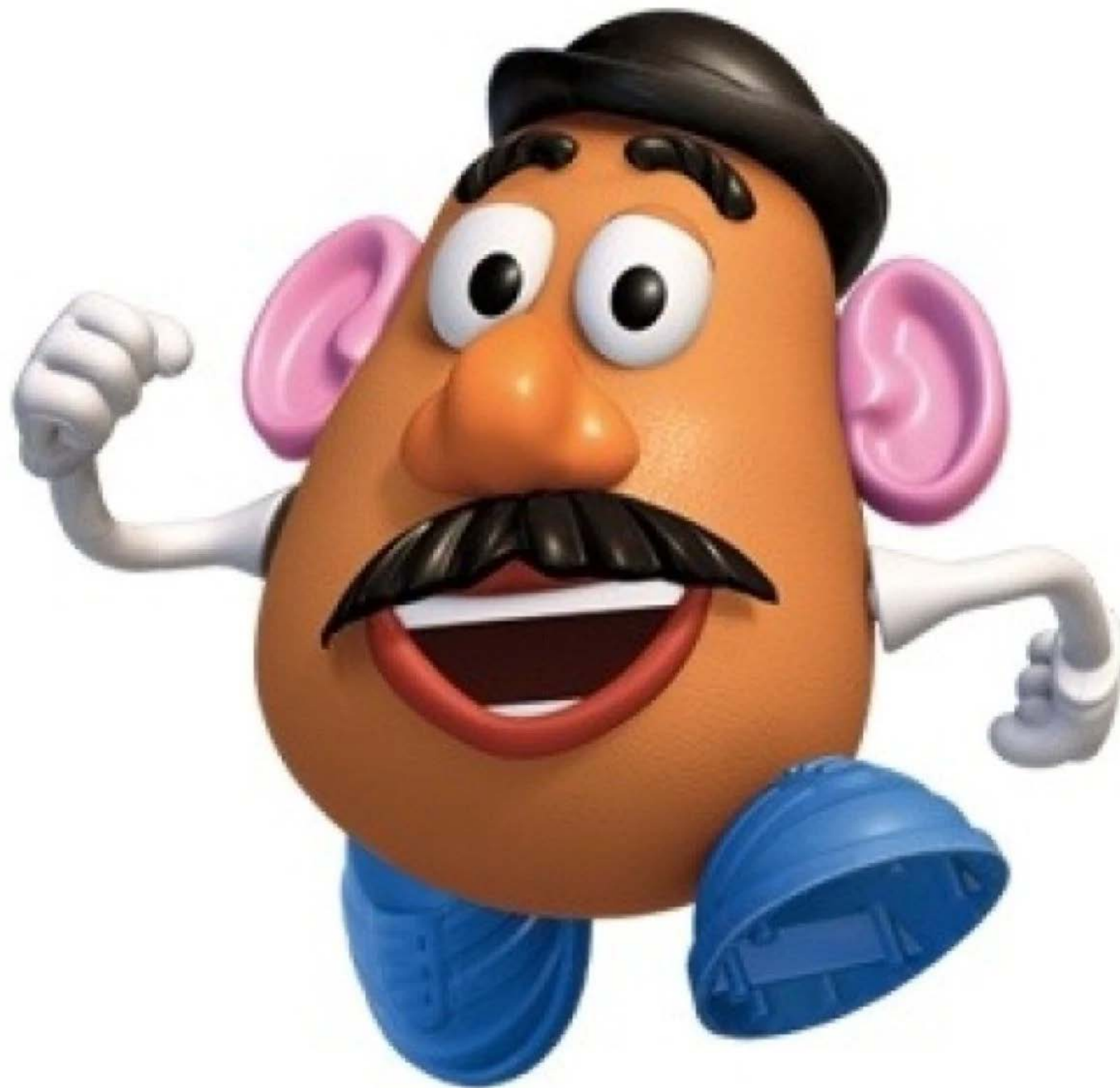












# What do they want....

# Canada Targeting

- Actors Targeting Canada

- TA516 [SmokingDro]
  - Very diverse actor who uses a variety of malware with pretty rudimentary tactics
  - Has recently been delivering Remocs
  - Exclusively using Password Protected docs since August
- TA564 [Captain Cha]
  - Originally found them targeting Poland, it's been all Canada since March
  - Performs Geogating
  - Delivered Nymaim to Poland and Danabot to Canada
- TA543 [Sagrid]
  - General Spammer/Trafficker
  - Deals in Ransoms, Bankers, Loaders
- TA545 [AirCanada]
  - Mainly targets Canada, sometimes Australia
  - Mainly delivers Stealers ZeroEvil and ARS this year
    - Seen delivering Meterpreter, QuesarRAT, AZORult, Panda Banker

- Targeted Brands


- AirCanada
- Bank of Montreal
- Canada Post
- Coast Capital Savings
- Interac
- Royal Bank of Canada
- Government of Canada

The image displays two screenshots of the Canadian Tax Refund portal. The top screenshot shows 'Step 1: Details' with a progress bar indicating four steps: 1. DETAILS (active), 2. PERSONAL INFORMATION, 3. FINANCIAL INFORMATION, and 4. CONFIRMATION. Below the progress bar, there is a 'Claim your Tax refund' section with a disclaimer. The bottom screenshot shows 'Step 3: Personal information' with a progress bar indicating four steps: 1. DISCLAIMER, 2. PERSONAL INFORMATION (active), 3. FINANCIAL INFORMATION, and 4. CONFIRMATION. Below the progress bar, there is a form to 'Enter your personal information' with fields for Title, First name, Last name, Social Insurance Number, Date of birth, Mother's maiden name, Address, Province, Postal code, and Telephone. A note states 'All data transmissions are held over 256-BIT secured SSL layer.' and 'Any fields marked with an asterisk (\*) are required.'

# TA564

☐

I'm not a robot

  
reCAPTCHA  
[Privacy](#) - [Terms](#)

Submit


## About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. [Why did this happen?](#)

IP address: [REDACTED]  
Time: 2019-03-19T20: [REDACTED]

☐

I'm not a robot

  
reCAPTCHA  
[Privacy](#) - [Terms](#)

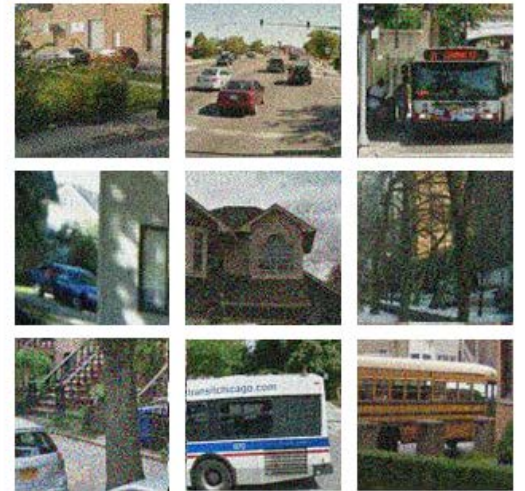
Submit

## About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. [Why did this happen?](#)

IP address: [REDACTED]  
Time: 2019-03-19T20: [REDACTED]

Select all images with  
**buses**

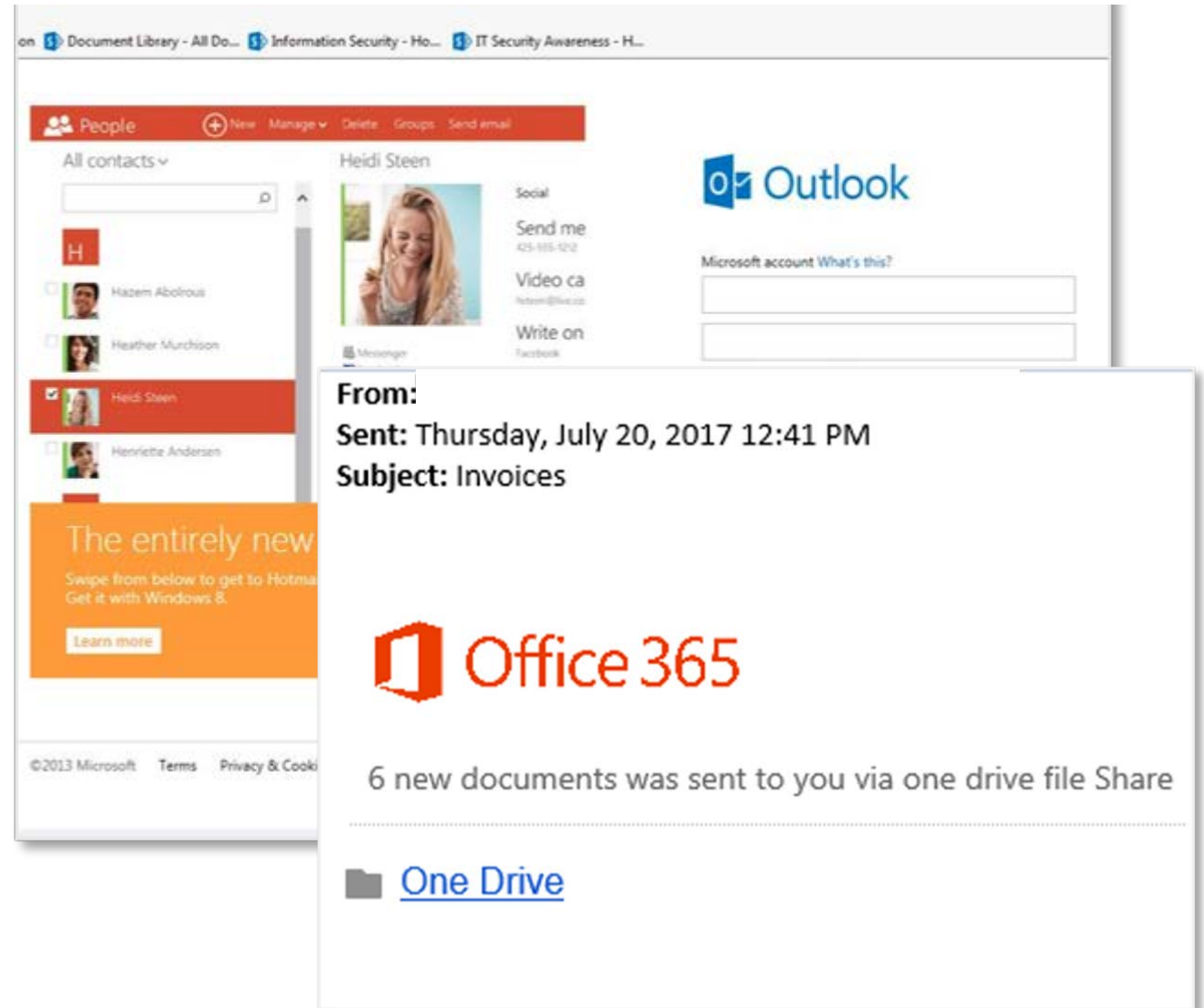


VERIFY



# Credential harvesting

- A single employee disclosing username and password was enough to spread the attack
- With access to our customer's user accounts, the attackers sent several massive phishing attacks from the compromised accounts making it harder for employees to recognize the attack since it was coming from a "real" email address
- The attack then spread through our environment



# Spear-phishing

- Targeted phishing attempt carefully designed to trick the regional VP Finance to execute on a payment from on behalf of customer “CEO”
- Customer domain spoofed to look very similar to customer email address and use of real emails
- Invoice had accurate details and email chain created a compelling story
- Attack could have costed our customer USD 292,000

Wed 5/31/2017 9:54 AM

Steven [redacted]  
Fwd: Invoice

You forwarded this message on 5/31/2017 12:30 PM.

Message [021185.pdf (42 KB)]

See below and find attached the due invoice for payment which should be received today or tomorrow at the latest. The express transfer charges

Please proceed with the payment and do furnish me with a bank payment slip

Best regards,  
Steven

Sent from my iPhone

----- Original Message -----  
From: [redacted]  
To: [redacted]  
Date: Mon, 5/31/2017 12:30 PM  
Subject: Invoice

Steve,

As discussed, please see attached the invoice which needs to be paid quickly as possible. I will send the documentation to you later.

Thanks in advance.

Scott

**WILLIAMS POPSON STI**  
SANAYI MAH. GAZIOSMANPASA  
AD. NO: 31/1, GUNGOREN,  
ISTANBUL, TURKEY  
T: +90 212 647 86 43  
F: +90 212 647 89 27

INVOICE  
INVOICE #: 021185  
Invoice Date: 24/05/2017

Supplier Corporate Address:  
**WILLIAMS POPSON STI**  
830 SANAYI MAH. GAZIOSMANPASA,  
CAD. NO: 31/1, GUNGOREN  
ISTANBUL, TURKEY

Billed To:  
[redacted]

Comments or Special Instructions: Prices are quoted in USD

Item #	Item Code	Description	Quantity	Unit Price	Total Price
1	3030	Mass Spectrometer GCHS-QP2020	1	\$96,500.00	\$96,500.00
2	700-90	Calweld 150-CH Crane Attachment Rig With 120' Kelly Bars	1	\$83,980.00	\$83,980.00
3	4206-1	Krupp HBS0 Hydraulic Percussion Drill Head	1	\$112,000.00	\$112,000.00

Shipping	\$0.00
<b>Total</b>	<b>\$292,480.00</b>

BANK NAME: TURKIYE I.S. BANKASI A.S  
BANK ADDRESS: KULELERI 34330, 4 LEVENT, ISTANBUL, TURKEY  
SWIFT: ISBKTRIS  
ACCOUNT NAME: WILLIAMS POPSON STI  
IBAN: TR10 0006 4000 0021 2970 0251 70

*[Signature]*

# Payroll scam

- Attempt to get payroll at customer to change “employee” direct deposit account
- Email sent from “employee’s” personal email to HR manager and, indirectly, to payroll administrator
- Employee happened to be a general manager

**From:** Chad [REDACTED]  
**Sent:** Tuesday, July 16, 2019 2:40 PM  
**To:** Sarah [REDACTED]  
**Subject:** Re: Direct deposit update

Find form attached. I want you to override any prenote to ensure the change made for the current pay cycle.

Thanks

**From:** Sarah [REDACTED]  
**Sent:** Tuesday, July 16, 2019 12:13 PM  
**To:** Salaried Payroll Department [REDACTED]  
**Subject:** [REDACTED] Direct deposit update  
**Importance:** High

Hello,

Please update Chad [REDACTED]'s Direct Deposit Account. See his email below and the supporting documents attached.

Please let me know when this has been complete.

**From:** Maria [REDACTED] <[REDACTED]@[REDACTED].com> On Behalf Of Salaried Payroll Department  
**Sent:** Tuesday, July 16, 2019 3:21 PM  
**To:** Chad [REDACTED] <[REDACTED]@[REDACTED].com>  
**Subject:** FW: [REDACTED] Direct deposit update  
**Importance:** High

Hi Chad

Just checking if this is yours because it was sent through personal email and not work email. Please confirm.

Thanks,

# Recommendations

# Be cyber-aware

- Security is no longer just about technology
- We all have an important role in securing our personal and work-related data





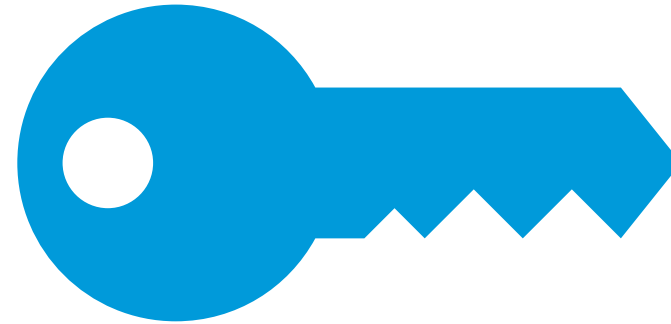
# Protect your inbox

- Beware of senders you don't know
- Hover over links before clicking
- Don't open attachments
- Report suspicious email



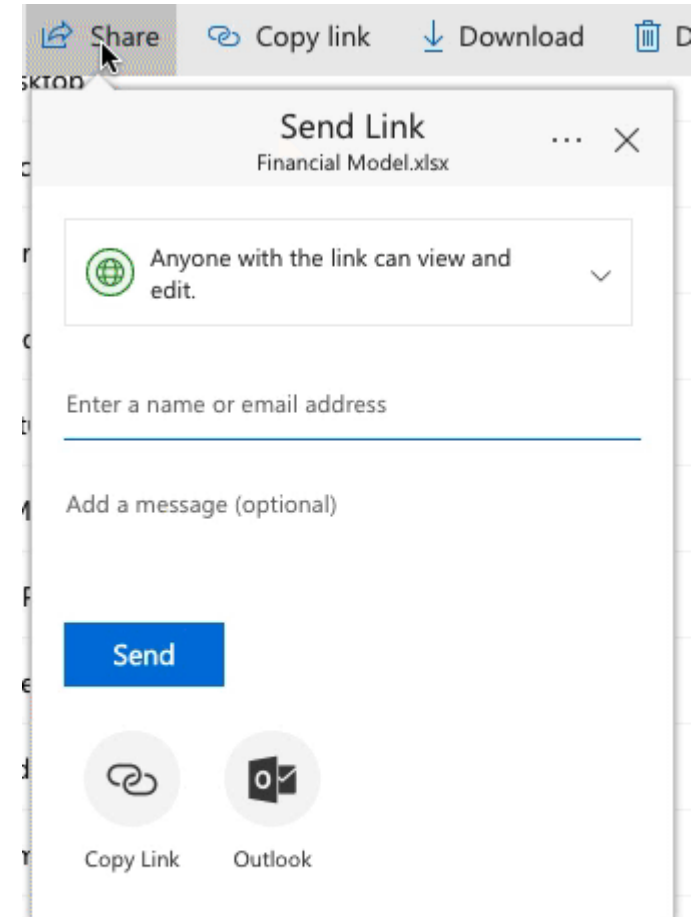
# Protect your identity

- Make your password difficult to guess – passphrases are a great option
- Consider a password manager (LastPass, Password Safe, and KeePass are some options)
- Enable multifactor authentication



# Protect your information

- Don't use USBs or other external devices
- Leverage cloud storage solutions when possible
- Manage permissions and expiration date



# Protect your device

- Check with your internet provider for free firewall and antivirus
- Ensure all software is up to date
- Limit data tracking
- Back up your data



A man and a woman are in a meeting room. The woman is pointing at a whiteboard covered in many colorful sticky notes. The man is holding a tablet and looking at the board. The background shows a large orange sculpture and a window with blinds.

# proofpoint®

## CC

CHANGE  
CHAMPIONS