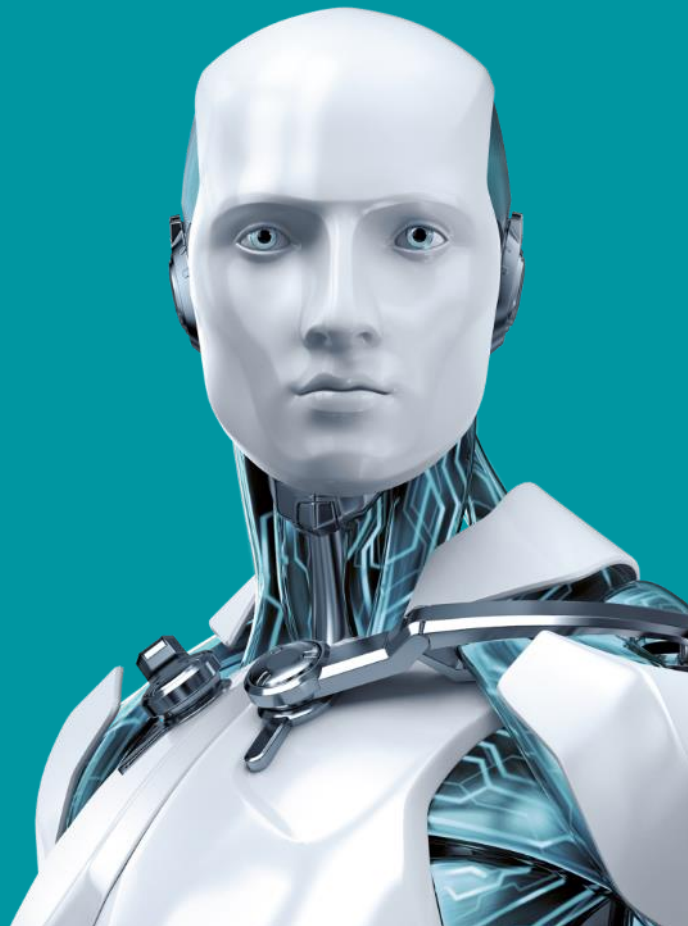
ESET CYBERSECURITY AWARENESS TRAINING

February 2022

ENJOY SAFER TECHNOLOGY™



Leonardo Corso
Presales Engineer at ESET Australia

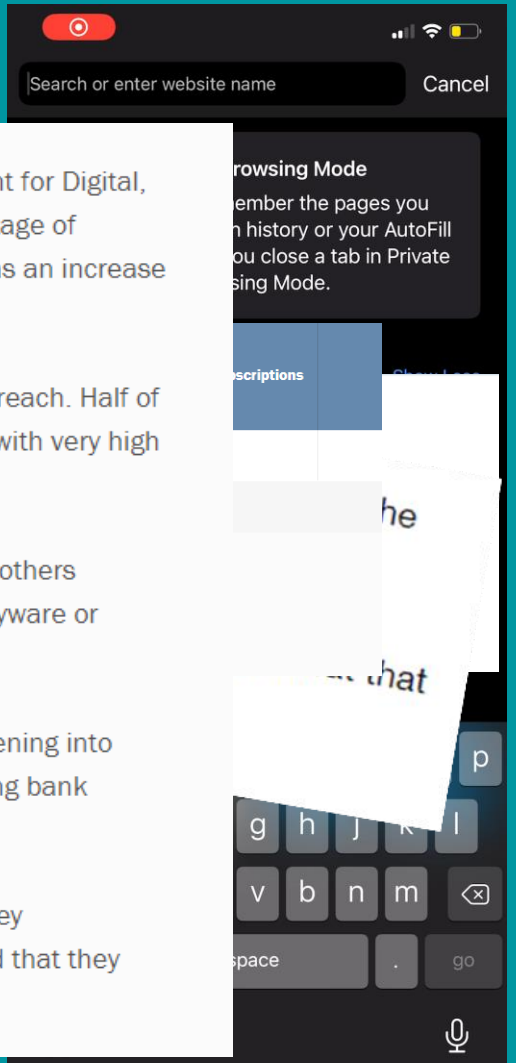
Luke Holland
Head Of Sales at ESET

Agenda

To show you best practices, tips and tricks to help you avoid being compromised / attacked.

1. Threats Overview
2. Password Safety
3. Web Protection
4. Email Protection

2020/21 Cyber – What has happened?



The Cyber Security Breaches Survey, published by the Department for Digital, Culture, Media and Sport last week, shows that while the percentage of charities reporting cyber breaches had remained stable, there was an increase in those charities using online donations and services.

Larger charities were more likely to say they had experienced a breach. Half of all high-income charities (£500,000 or more), and 68% of those with very high incomes (£5m or more) recorded breaches or attacks.

Nearly 80% of breaches involved phishing attacks, 23% involved others impersonating the charity's emails, and 16% involved viruses, spyware or ransomware.

Other less common types of breaches included unauthorised listening into video conferencing, taking over the charity's accounts and hacking bank accounts.

Of those charities that reported breaches, one in five said that they experienced an issue once a week. 18% of charities affected said that they end up losing money data or other assets.

ESET’s
Online Cybersecurity
Awareness Training

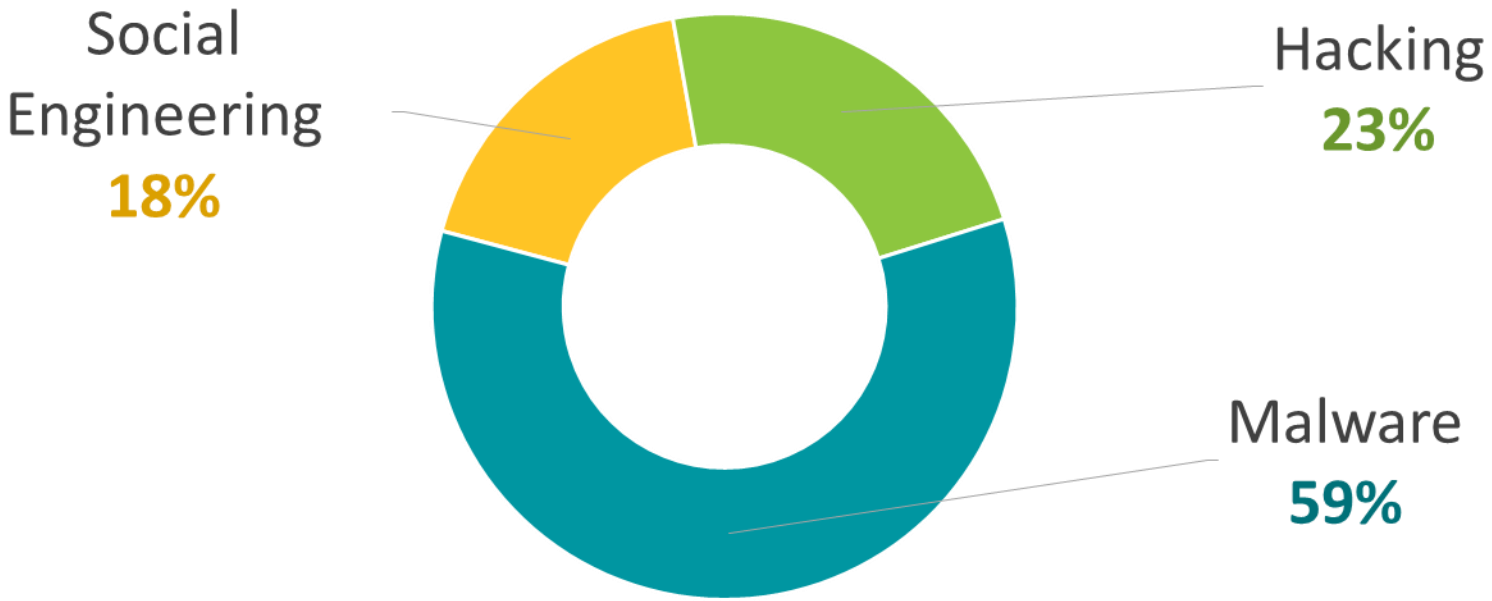
THREATS OVERVIEW

Root Cause of Data Breaches

Ponemon Institute 2020 Cost of Data Breach Study: Global Analysis

Data Breach Breakdown

Malicious Breaches Overview



Verizon 2020 Data Breach Investigations Report – specifically: incidents involving credentials

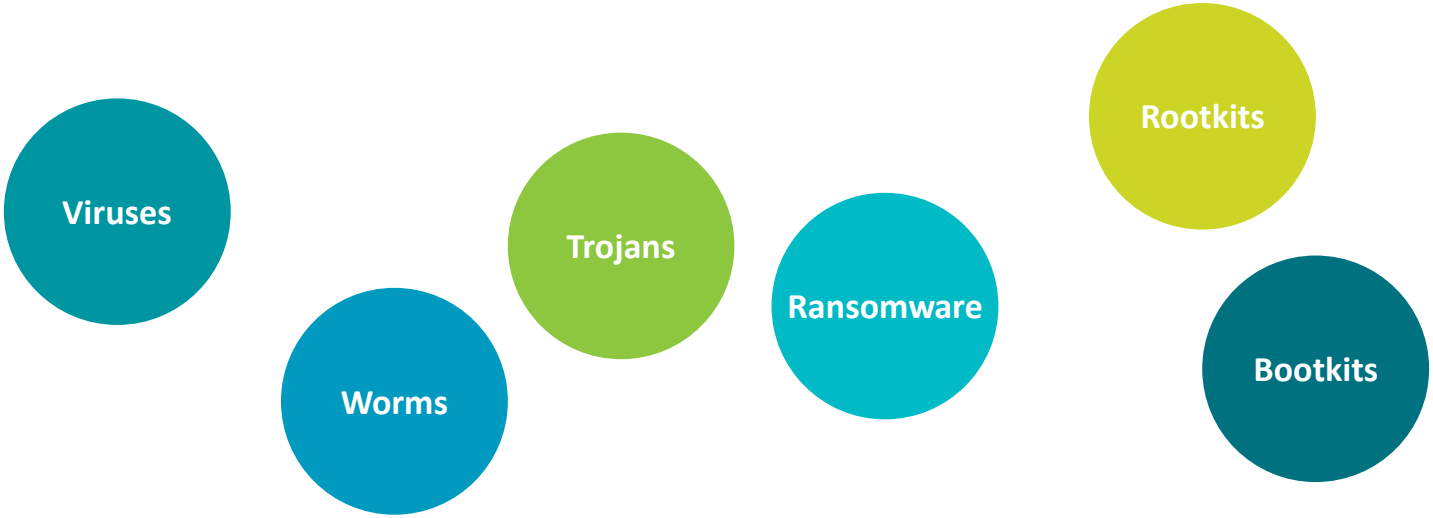
Threats Overview

Malware

Phishing

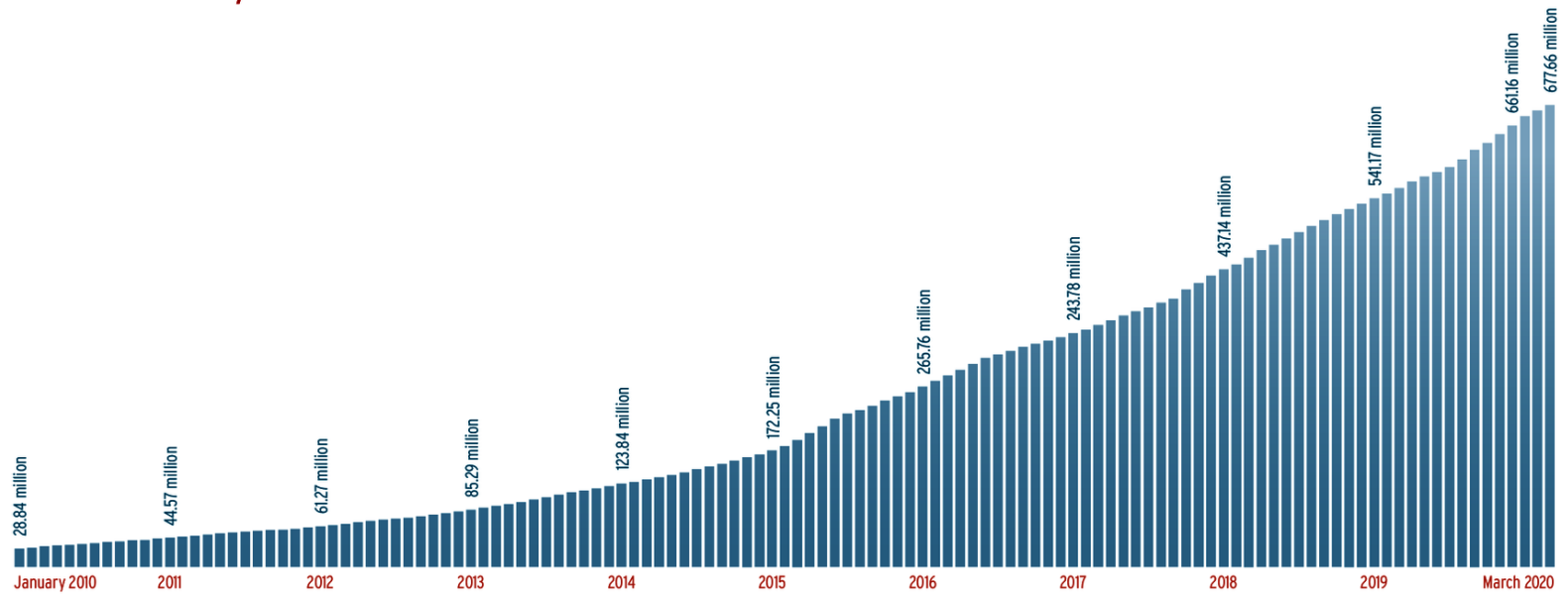
Social Engineering

Malware includes numerous threat families, all with different names.



Growth of Malware

AV-TEST
The Independent IT-Security Institute



Is malware on Windows only?

Is malware on mobile phones?

How does my computer and mobile get infected?

Top Tips to Avoid Malware

1. Install ESET Antivirus on all devices.
2. Be careful what you plug in.
3. Be careful what you click.
4. Get awareness training for entire family.

Threats Overview

Phishing

Phishing Stats

36% of people

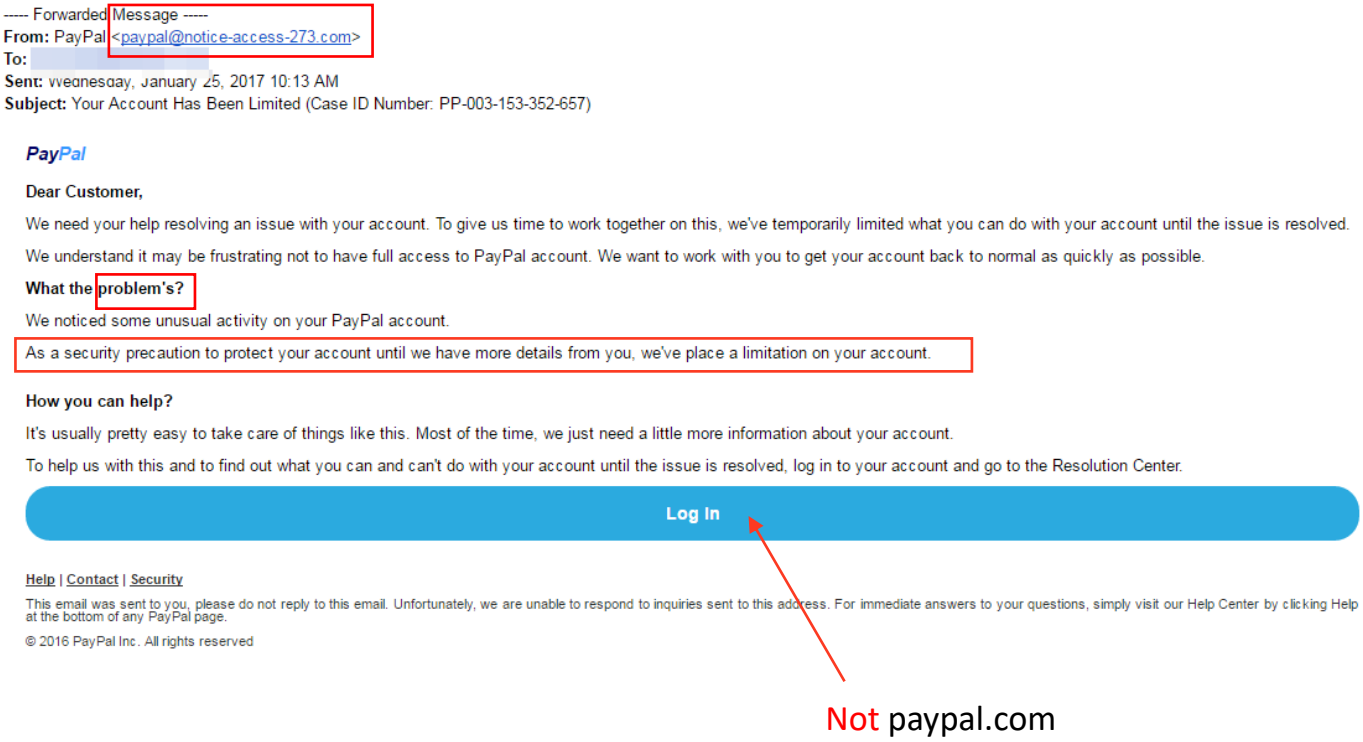
Open phishing messages
(32% last year)

16% of people

Open attachments
(14% last year)

Verizon 2020 Data Breach Investigations Report

Phishing Examples



----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

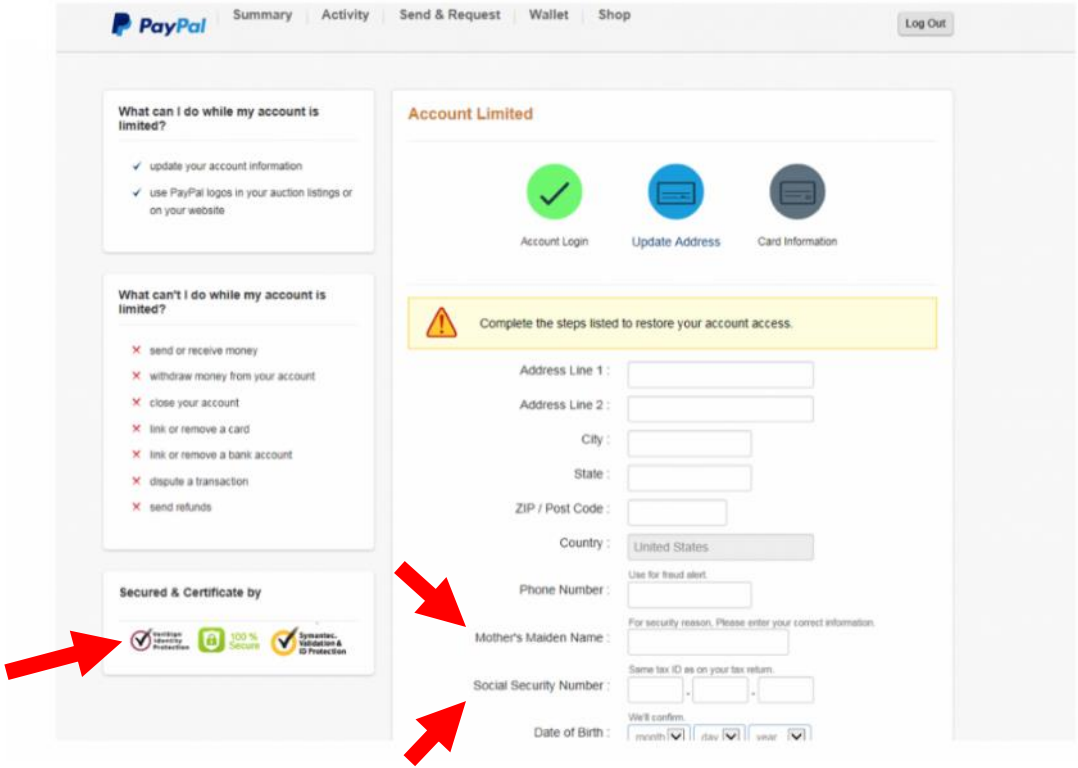
Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

Not paypal.com

Phishing Examples



Top Tips to Avoid Phishing

1. Check who the email sender is.
2. Check the email for grammar and spelling mistakes.
3. Mouse over the link to see where it goes.
4. Do not click the link – manually type it in.

Threats Overview

Social Engineering

Top Tips to Avoid Social Engineering

1. Be careful with the information you disclose.
2. Verify credentials of contractors.
3. If you have any doubts on the identity of callers, hang up and call their official company number back.

PASSWORD SAFETY

Poor Password Hygiene

Document or sticky note with passwords written on it

Poor Password Hygiene

Freely sharing password with friends, family members, colleagues

Poor Password Hygiene

8 characters = elephant

8 characters + 1 number = elephant1

8 characters + 1 number + 1 symbol = elephant1!

8 characters + 1 number + 1 symbol + 1 capital = Elephant1!

Poor Password Hygiene

elephant1!

elephant2@

elephant3#

elephant4$

Data breaches lead to password problems because…

- Passwords sometimes are extracted
- Very simple to try all alternative options of password-base

Example

- Password that was stolen was elephant
- Password required by website is 8 characters 1 symbol
- 32 symbols on the computer(would take a human 5 minutes)
- Computers can carry out these tasks in fractions of a second

Password Managers

Password Hygiene Checkup

https://haveibeenpwned.com/

- Currently checks 530 websites
- 11.2 billion compromised accounts contained

Top Tips for Password Safety

1. Utilize unique passwords across all websites/applications
2. Change your passwords often
3. Don’t share your password

INTERNET PROTECTION

Internet Protection Overview

Search Engine Safety

Top Tips for Search Engines

1. Stick to clicking on sites on the first page of results.
2. Be careful when clicking on non-name recognizable sites.
3. Malware commonly masquerades as free things.

Internet Protection Overview

Web Content Filter

Top Tips for Web Content Filter

1. Increase employee productivity by implementing a web filter.
2. Curb risky user behavior and reduce malware exposure by implementing a web filter.
3. Protect children’s mobile devices and computers from displaying inappropriate content with a web filter.

Internet Protection Overview

HTTPS

Top Tips for Secure Websites (HTTPS)

1. Before entering sensitive information, check to see if the site is secured by HTTPS.
2. Check to make sure this is a reputable website before entering credit card information; don’t just depend on the HTTPS indicator.

Internet Protection Overview

Public Wi-Fi

Top Tips for Public Wi-Fi

1. Verify the Wi-Fi name with the business owner prior to connecting.
2. Treat public Wi-Fi connections as compromised (unsafe).
3. Utilize an anti-malware product to help prevent against cyberattacks while connected.

EMAIL PROTECTION

Email Protection Overview

Spam Protection

ENJOY SAFER TECHNOLOGY™