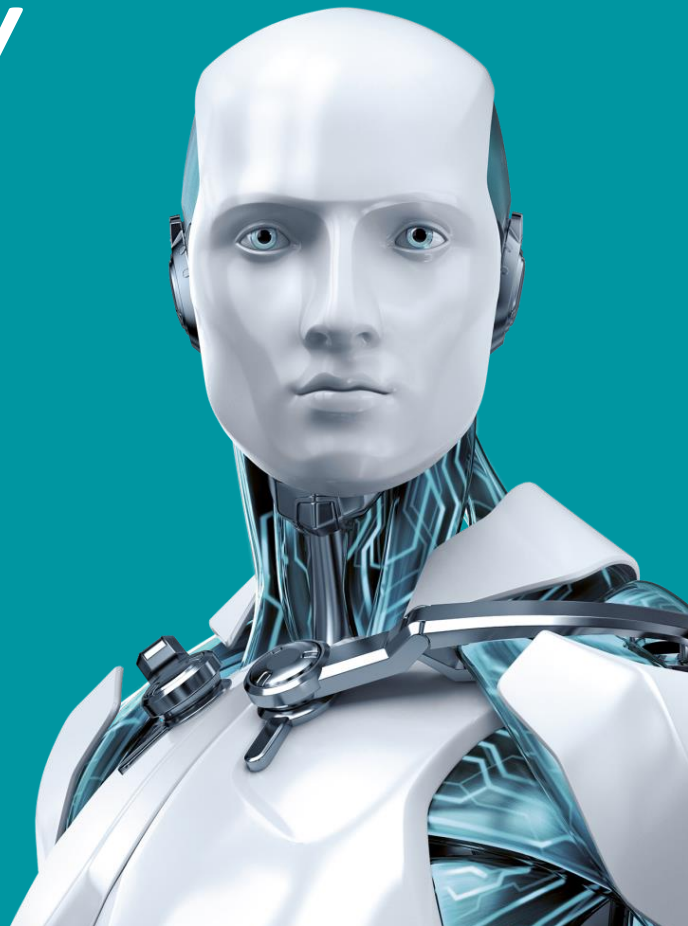
CYBERSECURITY AWARENESS TRAINING

PROVIDED FREE FOR VICTIMS OF ROMANCE SCAMS BY THE SOCIETY OF CITIZENS AGAINST ROMANCE SCAMS [SCARS]

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

eset® ENJOY SAFER TECHNOLOGY™



Agenda

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

- Threats Overview
- Password Safety
- Internet Protection
- Email Protection
- Preventive Measures

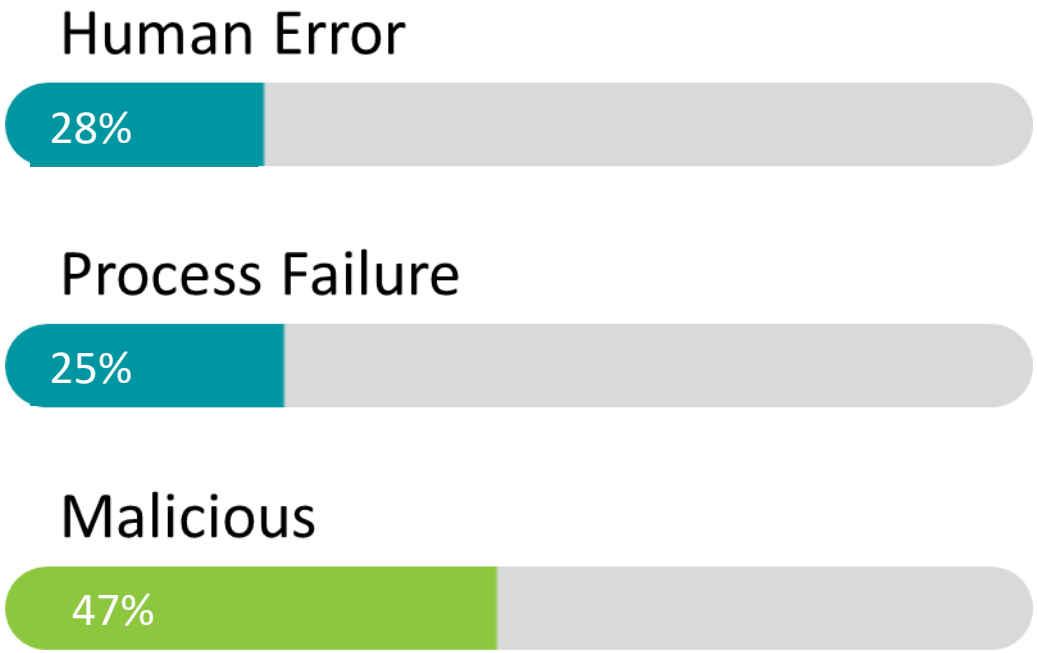
SCARS™

www.AgainstRomanceScams.org

Society of Citizens Against Romance Scams™

THREATS OVERVIEW

Root Causes of Data Breaches



Ponemon Institute 2017 Cost of Data Breach Study: Global Analysis

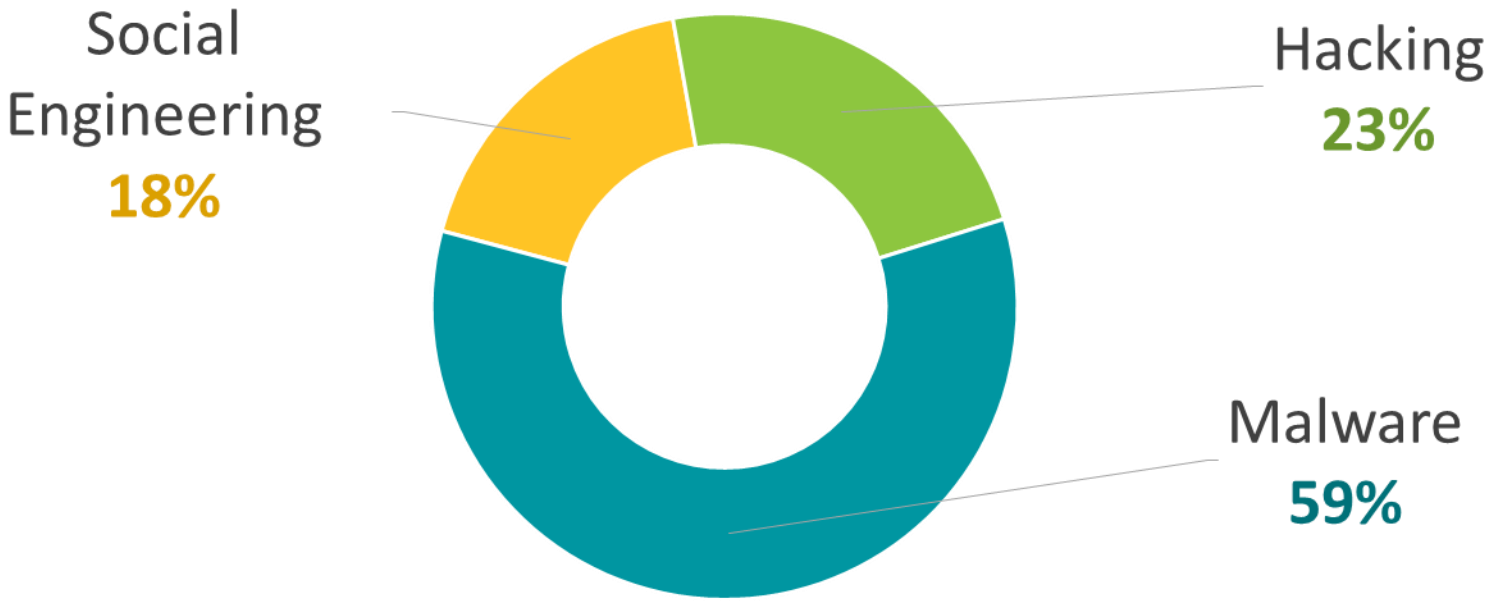
Data Breach Breakdown

Human Error

Verizon Data Breach Report 2016

Data Breach Breakdown

Malicious Breaches Overview



Verizon 2016 Data Breach Investigations Report – specifically: incidents involving credentials

Threats Overview

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

Malware

Phishing

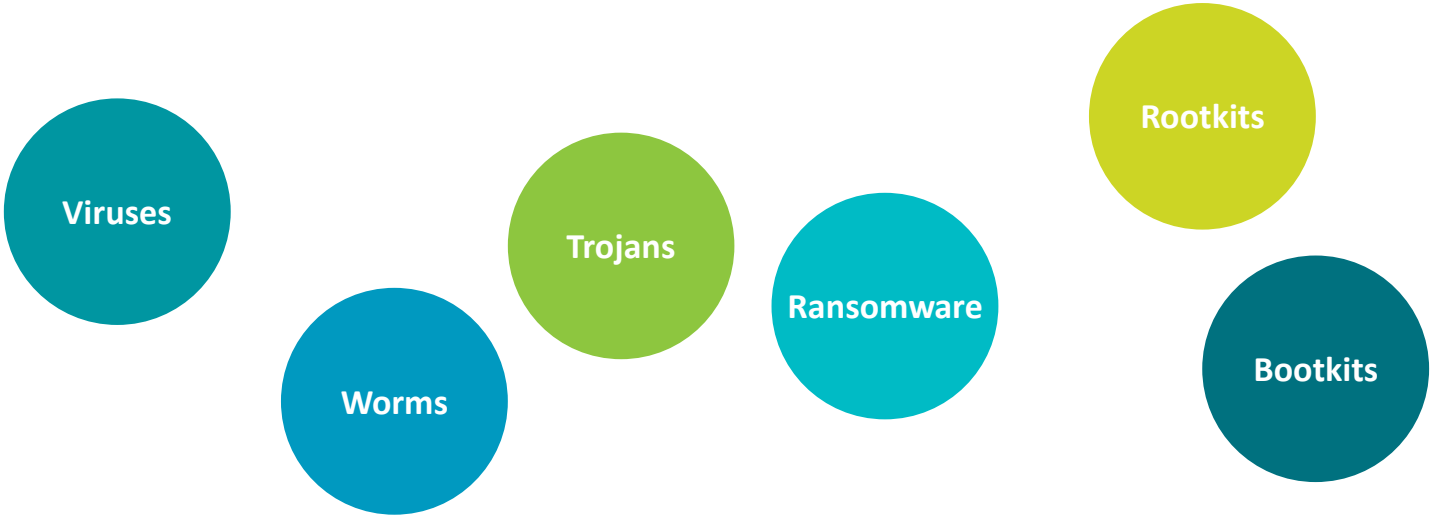
Social Engineering

Threats Overview

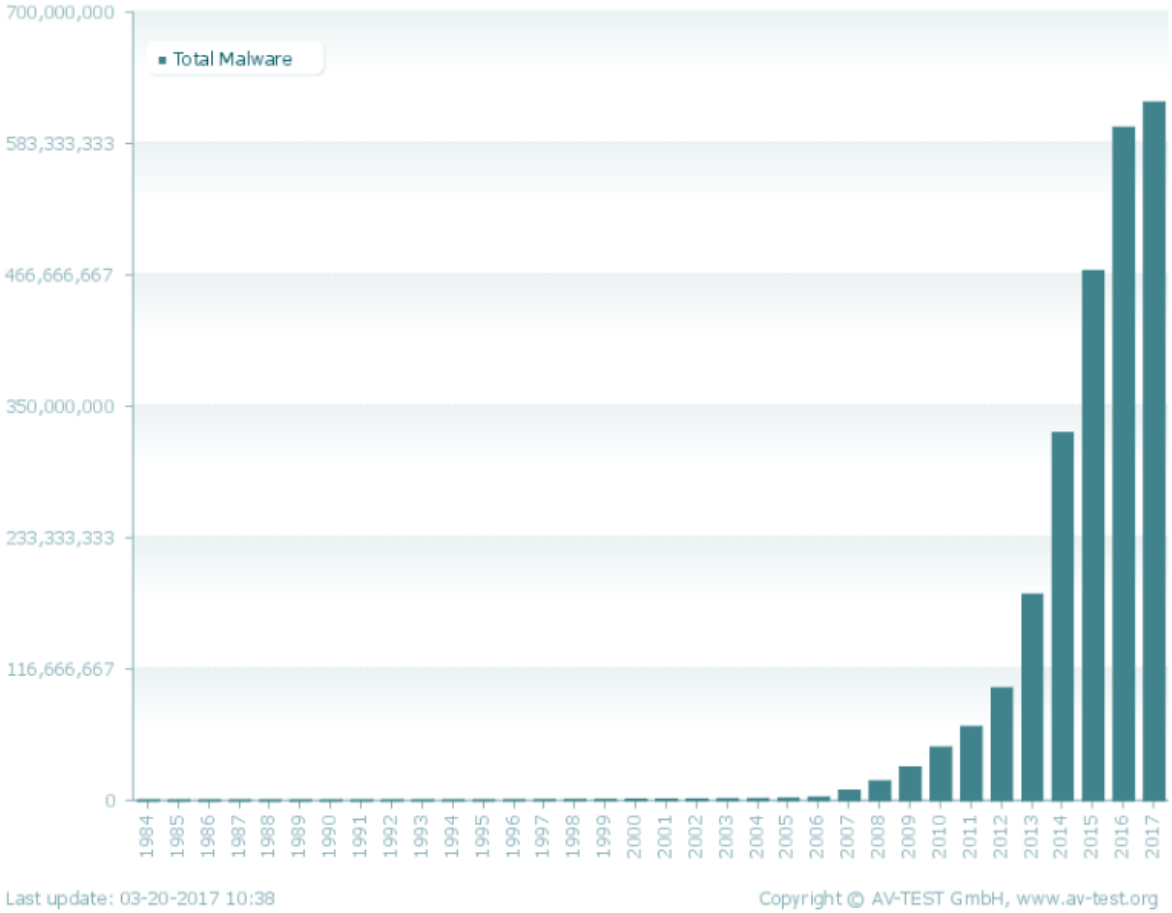
SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

Malware

Malware includes numerous threat families, all with different names.



Growth of Malware



Malware

- On average, 390,000 unique threats per day.[1]
- Unique threats ≠ extremely dissimilar.
- Malicious threats are changed in the smallest amount possible to evade detection.
- Malicious threats are targeted in order to have the highest penetration (success) rate.

[1]AV-TEST GmbH, www.av-test.org

Is malware on Windows only?

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Malware definitely exists on other operating systems (OSes) outside of Windows.
- Windows is typically the major target due to high market share.
- When new malware is released on other OSes, it typically has a high penetration rate due to people believing their Android, Mac, and Linux devices are safe without having any endpoint security installed.

Is malware on mobile phones?

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Mobile phone malware is a growing threat due to users doing the majority of their internet browsing on a cell phone.
- Ransomware, or screen locking malware, is a popular threat on mobile devices.
- In 2016, malware targeting Apple iOS (iPhones, iPads) increased. Apple doesn't allow vendors to create antivirus for these products, so users must depend on the company to fix any vulnerabilities.

How does my computer get infected?

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Clicking malicious links in email
- Plugging in an unknown flash drive
- Downloading malware masquerading as other software

How does my mobile device get infected?

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Clicking malicious links in email
- Downloading malware masquerading as other software
- Installing 3rd party apps directly from the internet instead of via official stores such as Google Play or Apple's App Store.

Top Tips to Avoid Malware

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

1. Install Endpoint Security 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

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

Phishing

Phishing? Or fishing?

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

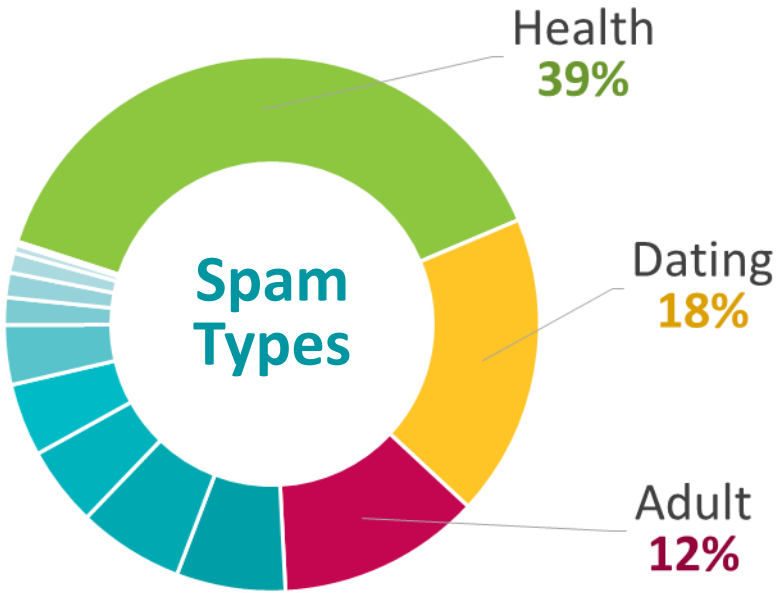
- Is the act of setting the bait (trap)…
- Casting it out into a wide ocean…
- Hoping that something bites that you can then hook.

Phishing

- Intentionally deceiving someone by posing as a legitimate company.
- Typically, utilizes email by pretending to be a company or service requesting you to do something.
- Hoping that you click the link and fill out the requested info.

Phishing Stats

- 54% of all inbound email is spam
- 1 in 20 email messages has malicious content



2016 Trustwave Global Security Report

Phishing Stats

30% of people

Open phishing messages
(23% last year)

12% of people

Open attachments
(11% last year)

Verizon 2016 Data Breach Investigations Report

Phishing Examples

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

----- 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.

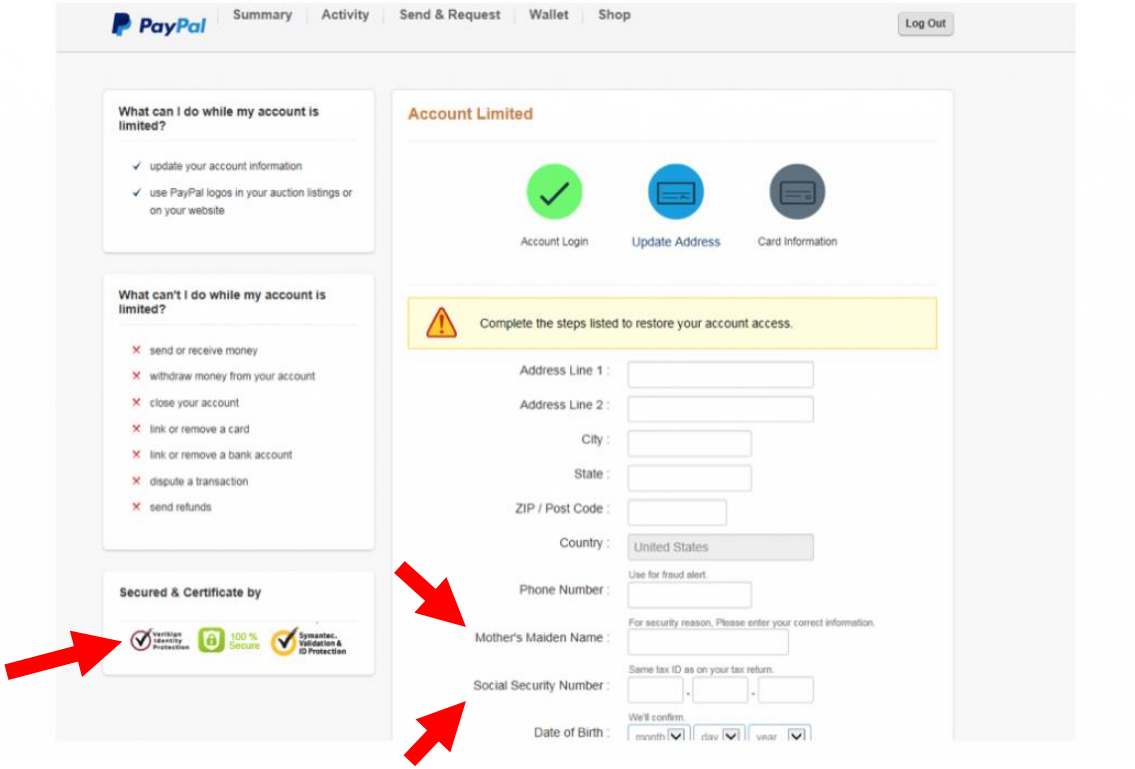
Log In

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.

Not paypal.com

Phishing Examples



Top Tips to Avoid Phishing

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

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

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

Social Engineering

Social Engineering

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Manipulation of people into divulging confidential or sensitive information
- Most commonly done over email, but also regularly carried out over the phone

Social Engineering

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Can be a slow gain of information
- Can attempt to gain all information needed at once

Social Engineering Examples

- Phone call targets employees at a business.
- Caller asks who the boss/CEO is.
- Requests his/her email address.
- Now the attacker has the username and the name of the person targeted for compromise.

Social Engineering Examples

- A person walks into office pretending to be a contractor.
- Due to his/her uniform, people assume it’s OK.
- Person walks into room with sensitive info and steals it.

Top Tips to Avoid Social Engineering

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

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.

SCARS™

www.AgainstRomanceScams.org

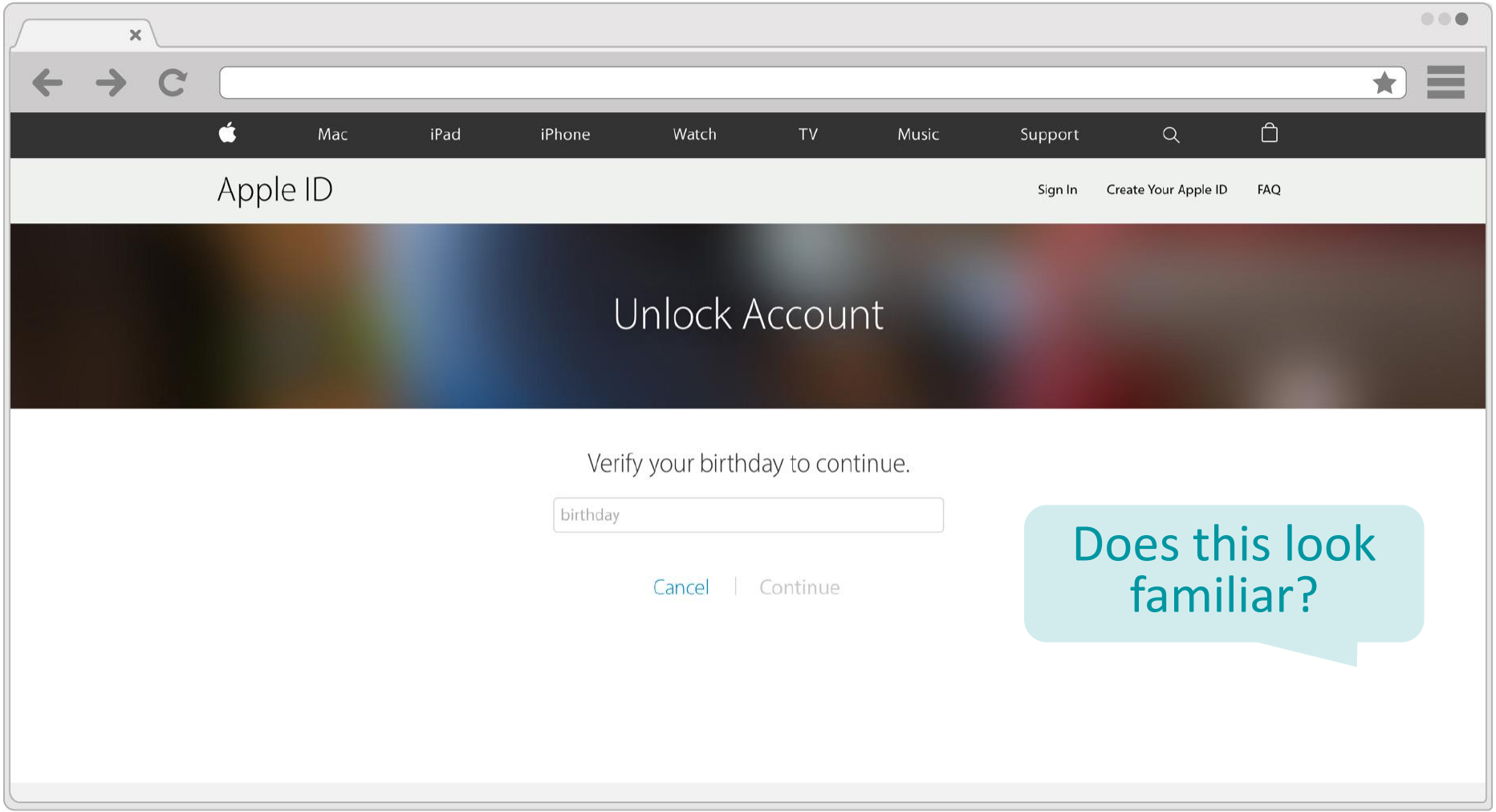
Society of Citizens Against Romance Scams™

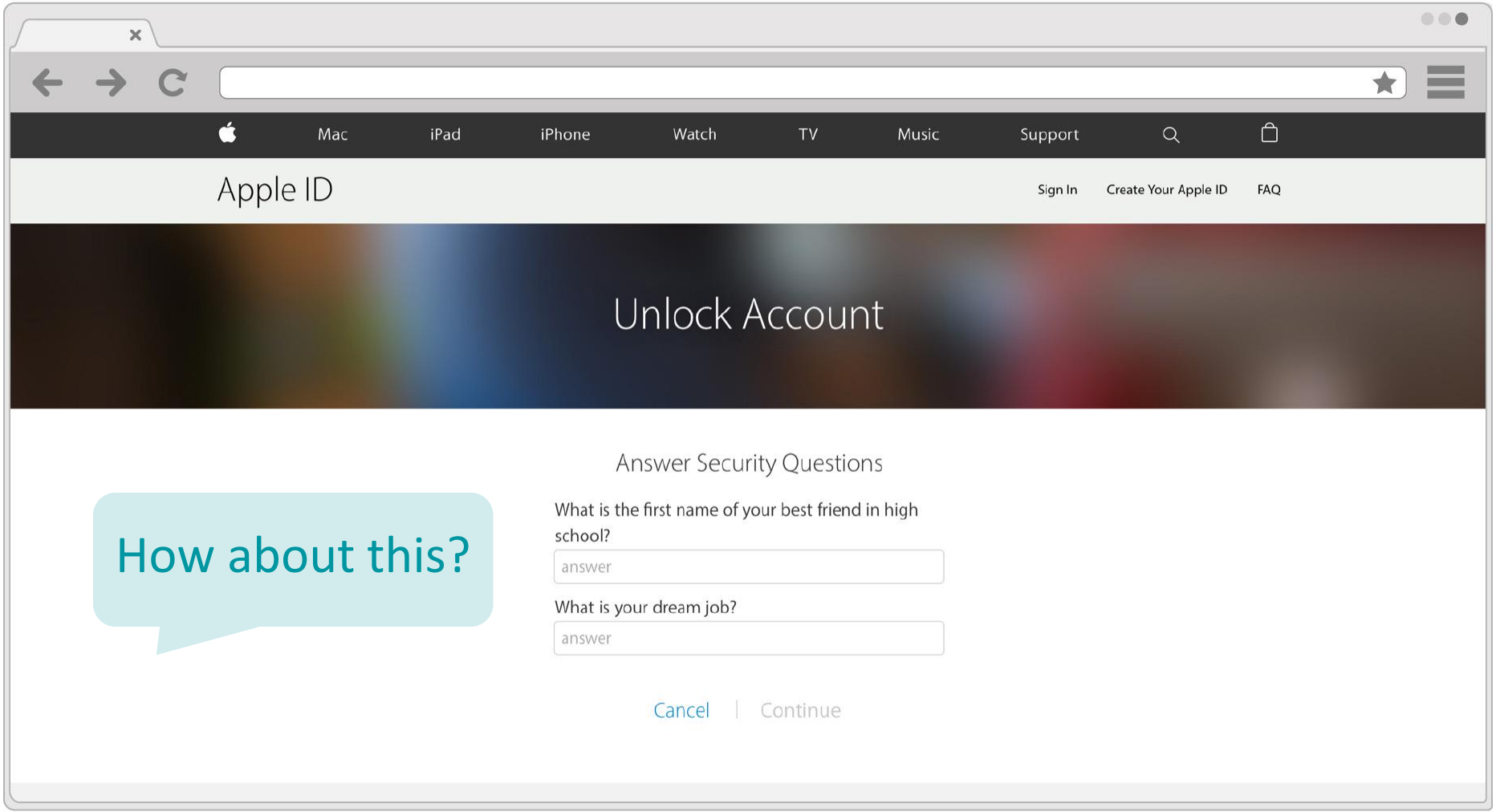
PASSWORD SAFETY

Can these answers be found on your Facebook account?

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- What city did you grow up in?
- What is your dog's name?
- What high school did you attend?
- What is your favorite book?
- What is your dream job?
- What is your mother's maiden name?


Mac
iPad
iPhone
Watch
TV
Music
Support
Apple ID
Sign In
Create Your Apple ID
FAQ
Unlock Account
Verify your birthday to continue.
birthday
Cancel
Continue
Does this look familiar?


Mac
iPad
iPhone
Watch
TV
Music
Support
Apple ID
Sign In
Create Your Apple ID
FAQ
Unlock Account
How about this?
Answer Security Questions
What is the first name of your best friend in high school?
answer
What is your dream job?
answer
Cancel
Continue

Security Questions

- Typically, users are honest when filling out security questions.
- Malicious parties can utilize social media to find out the answers to these questions, which allows them to reset your password.
- Best practice is to not be honest when filling out these questions. Treat security questions as another password field.

Users and Poor Password Hygiene

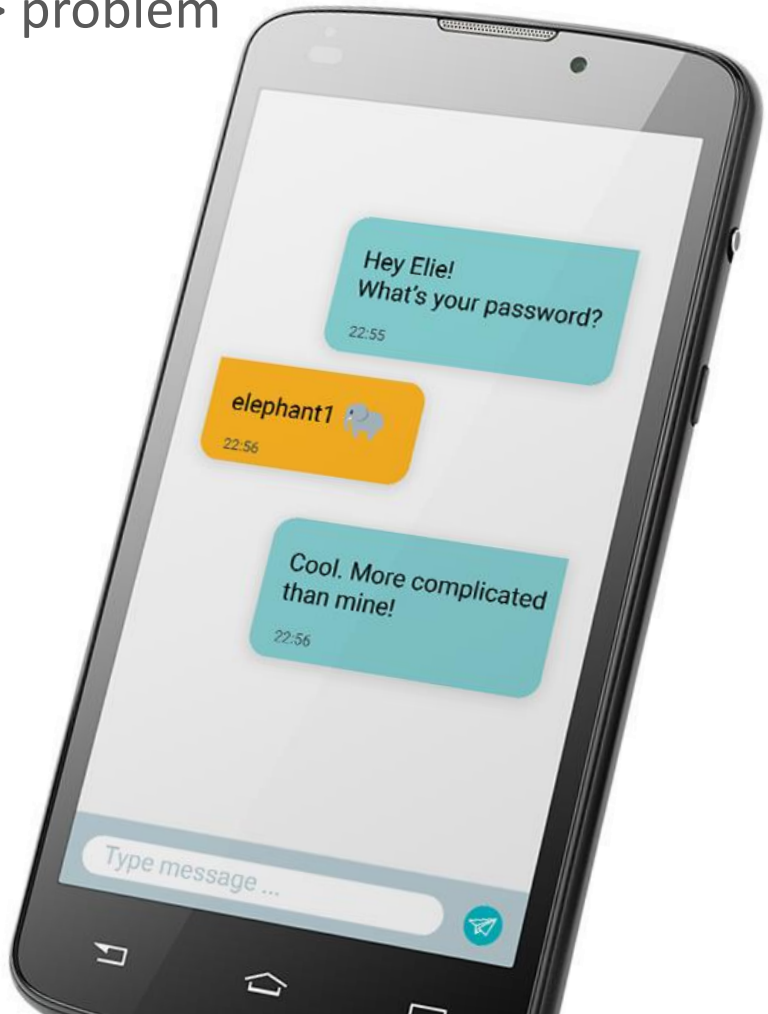
- Typically, users practice risky behavior with respect to passwords.
- Passwords nowadays can be a gateway into identity theft.

Access your data => problem

Document or **sticky note** with passwords written on it

Access your data => problem

Freely **share** passwords with friends, family members



Access your data => Problem

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

Elephant1!

8 characters

8 characters + 1 number

8 characters + 1 number + 1 symbol

8 characters + 1 number + 1 symbol + 1 capital

Access your data => problem

SCARS
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

Change password every 90 Days

Q1: elephant1!

Q2: elephant2@

Q3: elephant3#

Q4: elephant4$

Data breaches lead to password problems because…

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- 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

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

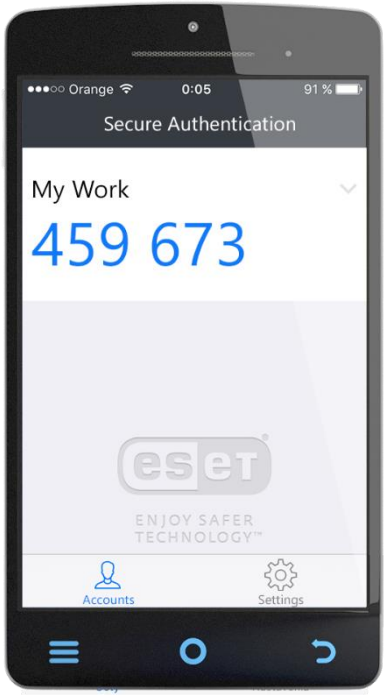
- If you have trouble remembering passwords or creating unique passwords, utilize a password manager.
- There are several very secure password managers on the market that work across all OSes.
- They will remember and auto-complete your passwords for you once your “master” password is entered.

Password Hygiene Checkup

https://haveibeenpwned.com/

- Currently checks 280 websites
- 5.0 billion compromised accounts contained
- Treat it like a credit-check

Two-factor Authentication (2FA) Explained



- As opposed to the standard password authentication, 2FA OTP (one-time password) uses two elements. These are *“something that user knows,”* such as a password or a PIN code, and *“something that user has,”* typically a mobile phone or hardware token.
- Used in combination, they provide greatly enhanced security for data access.

2FA solves the problem of:

- Data breach through weak or stolen passwords
- User-created passwords that are not random characters
- Re-use of passwords intended for access to company assets for private accounts
- Passwords containing user-specific data – e.g. name, date of birth
- Simple patterns to derive new passwords, such as “elephant1,” “elephant2,” etc.

Top Tips for Password Safety

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

1. Utilize unique passwords across all websites/applications
2. Enable and utilize 2FA on all websites that allow it
3. Choose unique, non-true security questions

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

INTERNET PROTECTION

Internet Protection Overview

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

Search Engine Safety

Web Content Filter

HTTPS

Public Wi-Fi

Internet of Things

Internet Protection Overview

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

Search Engine Safety

Search Engine Safety

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Nowadays, users utilize search engines to ask every question they can think of.
- Users click on search results without first checking if it is a legitimate site.
- This happens commonly on social media websites as well.

Search Engine Safety

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Even if the website is reputable, the advertisement being displayed could be malicious and infect your computer or mobile device.
- Free things (music, movies, game cheats, etc.) are very commonly filled with malware, and are rarely what they say they are.

Top Tips for Search Engines

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

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

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

Web Content Filter

Web Content Filter

- Filters web traffic based off pre-configured policies set by the administrator.
- There are both home versions and corporate versions.
- Home versions focus on child safety, while corporate versions focus on employee productivity.

Web Content Filter

- Not only can it restrict the content that is displayed to a certain audience, it can also be utilized to filter malicious content and protect the user.

Top Tips for Web Content Filter

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

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

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

HTTPS

HTTPS

- Is a protocol for secure communication over a computer network which is widely used on the internet
- HTTPS is typically notated by displaying a green lock in the web address bar:

HTTPS

- No sensitive information should be typed into a page that is not secured by HTTPS.
- Even though a page is secured with HTTPS, it does not automatically mean the page is safe.
- Most browsers have begun to let users know more easily when they are on a non-secure page.

Top Tips for Secure Websites (HTTPS)

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

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

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

Public Wi-Fi

Public Wi-Fi

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Is a non-secure network that users can connect to for free
- Typically found in hotels, coffee shops, libraries and many other places

Public Wi-Fi

- Do not assume that a network named “Library” is actually the wireless network for the Public Library.
- Verify with the business owner the name of their network.

Public Wi-Fi

- Is very insecure, so you should treat every public Wi-Fi connection as compromised (unsafe).
- This means you should not utilize any sensitive websites when connected (banking, social networking, etc.)
- If you need to access one of these sites, utilize your cell phone and do not connect it to Wi-Fi, just use the cell service.

Top Tips for Public Wi-Fi

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

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.

Internet Protection Overview

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

Internet of Things

Internet of Things (IoT)

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- This type of internet connection is convenient, but opens up a security hole that needs to be secured.
- Examples of IoT devices include internet-connected thermostats and closed circuit cameras.
- If you can connect to it from anywhere, that means anyone can – by simply guessing your password.
- Disable any web features that you do not utilize.
- Make sure all IoT devices are kept up to date.

Internet of Things (IoT)

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Routers are the first line of defense to protect IoT devices from exploitation.
- Routers should be immediately configured to change the default username and password to something unique.
- If someone gains access to your router they can see all other devices on your network.
- Make sure your router is regularly updated to avoid exploitation.

Top Tips for Internet of Things (IoT)

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

1. Change default usernames and passwords on all devices including routers.
2. If you do not utilize the web features, disable them.
3. Make sure all IoT devices, including routers, are kept up to date with the newest firmware.

SCARS™

www.AgainstRomanceScams.org

Society of Citizens Against Romance Scams™

EMAIL PROTECTION

Email Protection Overview

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

2FA

Password Reset

Spam Protection

Attachment Policy

Email Protection Overview

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

2FA

2FA (Two-Factor Authentication) and Email

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Email is most important account needing protection, because if someone gains access to your email, they can utilize the password reset function to gain access to other services.
- As we mentioned earlier, 2FA is a great way to protect your email from being compromised.

2FA and Email

- Most major email providers allow you to set up 2FA with your email account.
- Once set up, the attacker would need your password and your cell phone in order to break into your email account.

Top Tips for 2FA and Email

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

1. Password protect or utilize fingerprint reader to protect your 2FA app in case of a lost device.
2. Do not utilize SMS if you can help it as a 2FA method; always use an application or push.
3. Enable 2FA not just on email but all critical websites and applications that allow it.

Email Protection Overview

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

Password Reset

Password Reset

- When passwords are forgotten, the ability to reset your password is very convenient, but if not utilized properly this can allow someone to easily take over your account.

- Some websites do not require any security questions to be answered, nor require any additional information besides account email address to initiate a password reset.

Password Reset

- Usually when someone requests a password reset, an email is sent to the email address on file with this information.
- Monitor these emails and contact the vendor directly if you see these and did not initiate them yourself. (But remember the spam/phishing rules from earlier.)

Top Tips for Password Reset

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

1. Utilize strong unique passwords.
2. Utilize strong, not correct, security questions.
3. Monitor attempted password resets on your accounts for fraudulent activity.

Email Protection Overview

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

Spam Protection

Spam Protection

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Everyone gets spam; even with the best protection, some still slips through the cracks.
- Some email providers have better spam protection than others.
- A third party anti-spam product can supplement protection provided by the email provider.

Spam Protection

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Never open spam emails, even if you think it is funny to see the content inside.
- Never respond to spam emails.
- Be careful using your email address to sign up for contests or enter websites.
- When posting your email to a public website, always add special breaks in your email address. Example: ben(at)eset dotcom

Top Tips for Spam Protection

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

1. Utilize a different provider or 3rd party product if necessary.
2. Never click, open, or respond to spam messages.
3. When posting email to classified sites, use the following format to keep spam bots from retrieving and using your address: john.smith (at) email.com.

Email Protection Overview

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

Attachment Policy

Attachment Policy

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams

- Attachments are one of the most common ways to get viruses or malware.
- Even though an attachment might look like a document or Excel file, it might contain a virus or malware.

Attachment Policy

- Rules should be in place at your company to prevent receiving certain types of attachment files.
- Employees should receive training that describes why attachments can be harmful.
- Never open attachments from unknown senders.
- If you see something that is questionable, send to your IT department for verification.

Top Tips for Attachment Policies

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

1. Combine training with a clear attachment policy for employees.
2. Never open or save attachments from an unknown sender.
3. Even though something looks like a file that you do not think is malicious, doesn't mean it isn't malicious.

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

PREVENTIVE MEASURES

Top Tips for Preventive Measures

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

1. Utilize an ANTIVIRUS product on all devices, not just Windows computers.
2. Define a clear attachment policy coupled with a spam filter.
3. Implement a Web content filter to help with malicious content, inappropriate content, and productivity issues.
4. Utilize unique passwords and maintain a clear password policy. If needed, use a password manager.
5. Keep all internet-connected devices up to date, including routers, IoT devices, computers, mobile devices.

To Learn More About Online Scams Visit
www.RomanceScamsNow.com

Romance SCAMS Now.com™©

ESET® ENJOY SAFER TECHNOLOGY™

SCARS™
www.AgainstRomanceScams.org
Society of Citizens Against Romance Scams™

PROVIDED FREE FOR VICTIMS OF ROMANCE SCAMS BY THE SOCIETY OF CITIZENS AGAINST ROMANCE SCAMS [SCARS]
www.AgainstRomanceScams.org