Information Security Awareness

October 31, 2024

Solutions for **Success**

POINT ALLIANCE

Agenda

- Introduction
- The Threat Landscape
- Security Tips
  - 10 Common Traits of Phishing
  - Securing the sign-in process
  - Tech support scam
  - Working more securely while travelling
- Next steps
- Resources
- Questions

John Zarei

- Point Alliance
- john.zarei@pointalliance.com
- http://linkedin.com/in/johnzarei

Point Alliance

- Microsoft Solutions Partner w/Modern Work & Security Designations
- Microsoft Gold Partner with 11 Competencies (legacy)
- 100% Microsoft Certified Team
- pointalliance.com/companyprofile

POINT ALLIANCE
EST. 2002
SOLUTIONS FOR SUCCESS

Microsoft Solutions Partner
Security

Microsoft Solutions Partner
Modern Work

Security is critical for your business

Businesses are experiencing an increase in both the volume and sophistication of cyberattacks.

As data has proliferated and more people work and connect from anywhere, bad actors have responded by developing sophisticated methods for gaining access to your resources and stealing data, sabotaging your business, or extorting money.

An *effective* cybersecurity program includes **people, processes, and technology** solutions that *together* reduce the risk of business disruption, financial loss, and reputational damage from an attack.

Every year the number of attacks increases, and adversaries develop new methods of evading detection.

300% Increase in ransomware attacks

23% Experienced a security breach

USD$108K Average cost to businesses

The Threat Landscape

DIGITAL

IN-PERSON

PHONE

The Digital Threat Landscape

EMAIL PHISHING

SPEAR PHISHING

CLONE PHISHING

WHALING

POP-UP PHISHING

- Email phishing is when scammers create emails that impersonate legitimate companies and attempt to steal your information.
- Spear phishing is similar to email phishing, but the messages are more personalized. For example, they may appear to come from your boss.
- Clone phishing is when scammers replicate an email you have received, but include a dangerous attachment or link.
- Whaling is when scammers target high-ranking executives to gain access to money or sensitive data.
- Pop-Up phishing is when fraudulent pop-ups trick users into installing malware.

The In-Person Threat Landscape

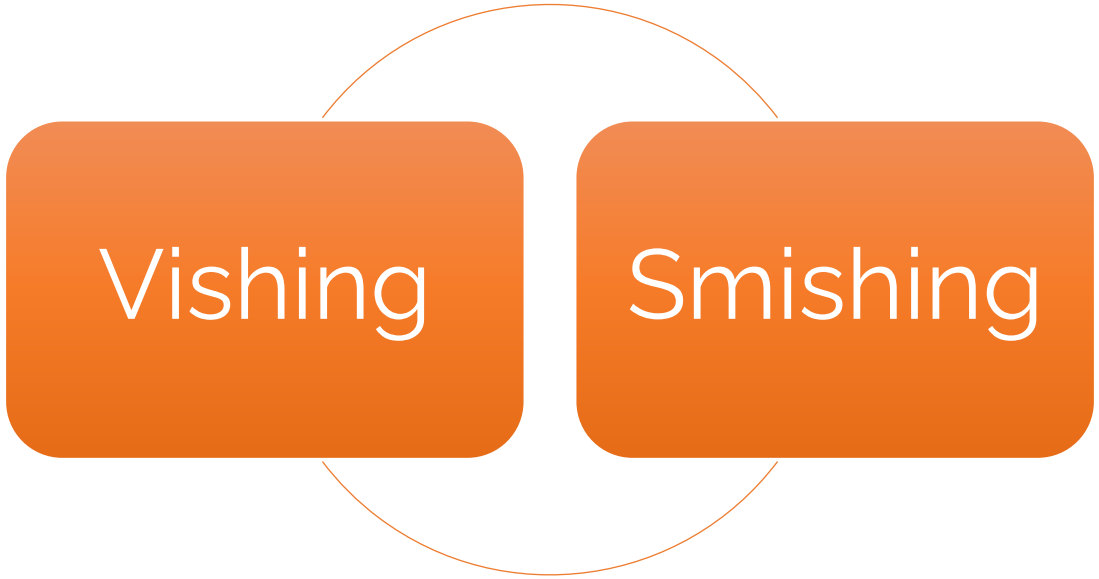
- USB attacks occur when a USB stick carrying malware is given to someone or is left in a public area. Eventually, that USB may be found and plugged into a device, causing it to become infected.
- Tailgating refers to someone who – without the proper authentication – follows an authenticated employee onto premises. The attacker might impersonate an employee, delivery driver or befriend an employee outside of the building to pretext the situation.

USB Attacks

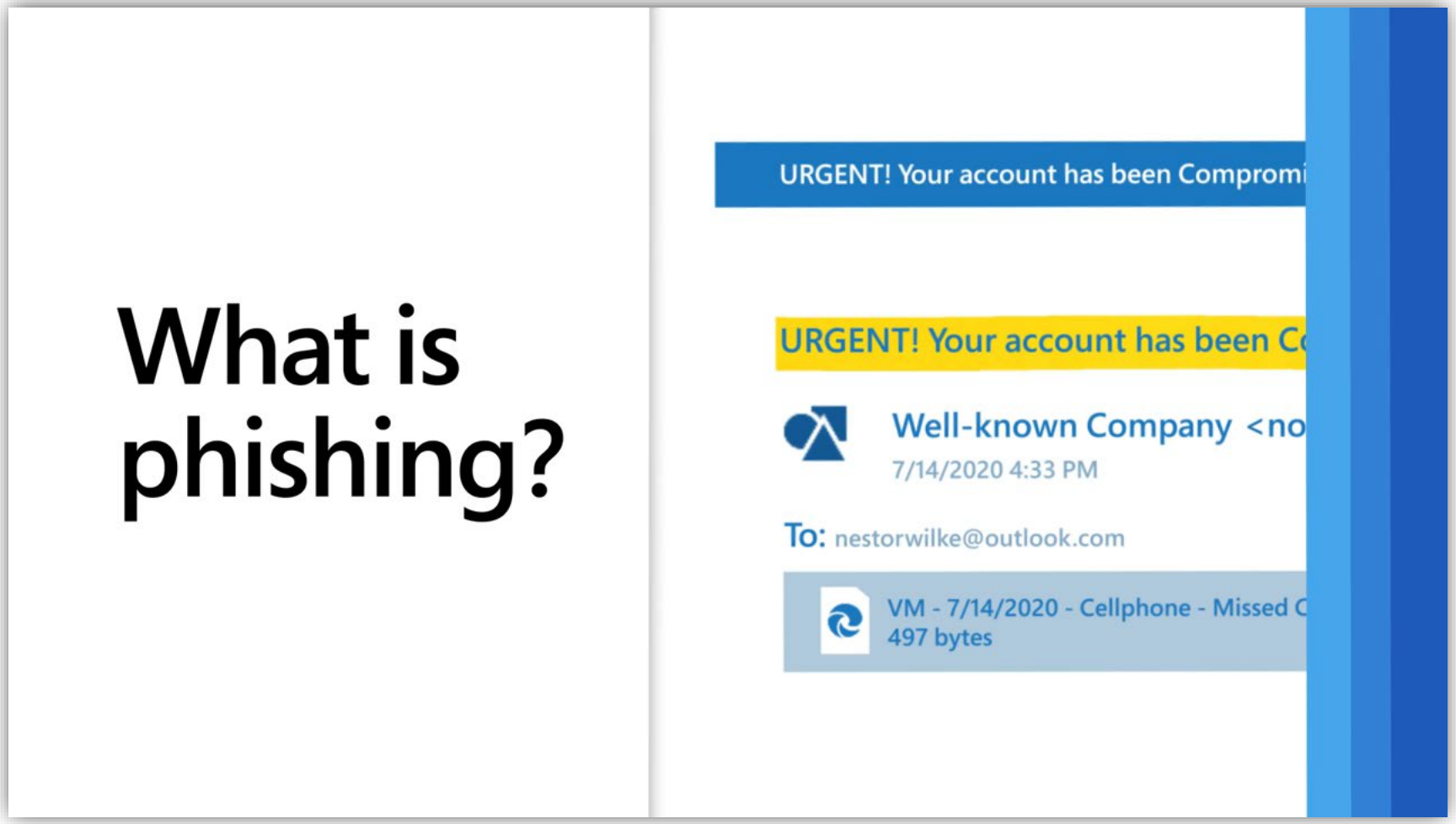
Tailgating

The Phone Threat Landscape

- Vishing is phishing attempted via phone call (e.g. a 'bank' needing your SIN, credit card, or bank account number.
- Smishing is phishing attempted via SMS messenger using infected links.



What is phishing?



10 Common Traits of Phishing

1. Asking for Personal Info.
2. Inconsistencies in Links
3. Unrealistic Threats
4. Generic Greetings
5. A Sense of Urgency
6. You're Asked to Send Money
7. Too Good to be True
8. Poor Spelling & Grammer
9. Suspicious Attachments
10. From Government Agency

10 Common Traits of Phishing

1. **Asking for Personal Info.**
2. Inconsistencies in Links
3. Unrealistic Threats
4. Generic Greetings
5. A Sense of Urgency
6. You're Asked to Send Money
7. Too Good to be True
8. Poor Spelling & Grammer
9. Suspicious Attachments
10. From Government Agency

Most reputable organizations will never email you asking for your address, phone number, or other personal data.

10 Common Traits of Phishing

1. Asking for Personal Info.
2. **Inconsistencies in Links**
3. Unrealistic Threats
4. Generic Greetings
5. A Sense of Urgency
6. You're Asked to Send Money
7. Too Good to be True
8. Poor Spelling & Grammer
9. Suspicious Attachments
10. From Government Agency

Always hover over links with your mouse pointer to display the full URL. If it leads somewhere that doesn't logically belong within the context of the email, or generally looks nonsensical, **don't click!**

10 Common Traits of Phishing

1. Asking for Personal Info.
2. Inconsistencies in Links
3. **Unrealistic Threats**
4. Generic Greetings
5. A Sense of Urgency
6. You're Asked to Send Money
7. Too Good to be True
8. Poor Spelling & Grammer
9. Suspicious Attachments
10. From Government Agency

Phishing emails often feature **threating language**, such as "PAYMENT OVERDUE!" or "Your account has been compromised", in order to generate a response.

10 Common Traits of Phishing

1. Asking for Personal Info.
2. Inconsistencies in Links
3. Unrealistic Threats
4. **Generic Greetings**
5. A Sense of Urgency
6. You're Asked to Send Money
7. Too Good to be True
8. Poor Spelling & Grammer
9. Suspicious Attachments
10. From Government Agency

Unlike legitimate entities that will address you by your full name or surname, **phishing emails usually opt for generic greetings** such as Dear Employee or Dear Madam/Sir.

10 Common Traits of Phishing

1. Asking for Personal Info.
2. Inconsistencies in Links
3. Unrealistic Threats
4. Generic Greetings
5. **A Sense of Urgency**
6. You're Asked to Send Money
7. Too Good to be True
8. Poor Spelling & Grammer
9. Suspicious Attachments
10. From Government Agency

Similar to unrealistic threats, emails that urge you to click to a link or download an attachment or update your account immediately are likely scam.

10 Common Traits of Phishing

1. Asking for Personal Info.
2. Inconsistencies in Links
3. Unrealistic Threats
4. Generic Greetings
5. A Sense of Urgency
6. **You're Asked to Send Money**
7. Too Good to be True
8. Poor Spelling & Grammer
9. Suspicious Attachments
10. From Government Agency

Whether it be overdue taxes or an upfront payment to cover expenses, **any emails that asks for money should be immediately raise your suspicious**.

10 Common Traits of Phishing

1. Asking for Personal Info.
2. Inconsistencies in Links
3. Unrealistic Threats
4. Generic Greetings
5. A Sense of Urgency
6. You're Asked to Send Money
7. **Too Good to be True**
8. Poor Spelling & Grammer
9. Suspicious Attachments
10. From Government Agency

The old saying remains true to this day: **if it's too good to be true, it's likely untrue**. Keep that in mind anytime you get an email claiming you won the lottery or are due a large family inheritance.

10 Common Traits of Phishing

1. Asking for Personal Info.
2. Inconsistencies in Links
3. Unrealistic Threats
4. Generic Greetings
5. A Sense of Urgency
6. You're Asked to Send Money
7. Too Good to be True
8. **Poor Spelling & Grammer**
9. Suspicious Attachments
10. From Government Agency

Most generic phishing attempts contain spelling and **grammar errors or feature awkward wording/phrasing**.

10 Common Traits of Phishing

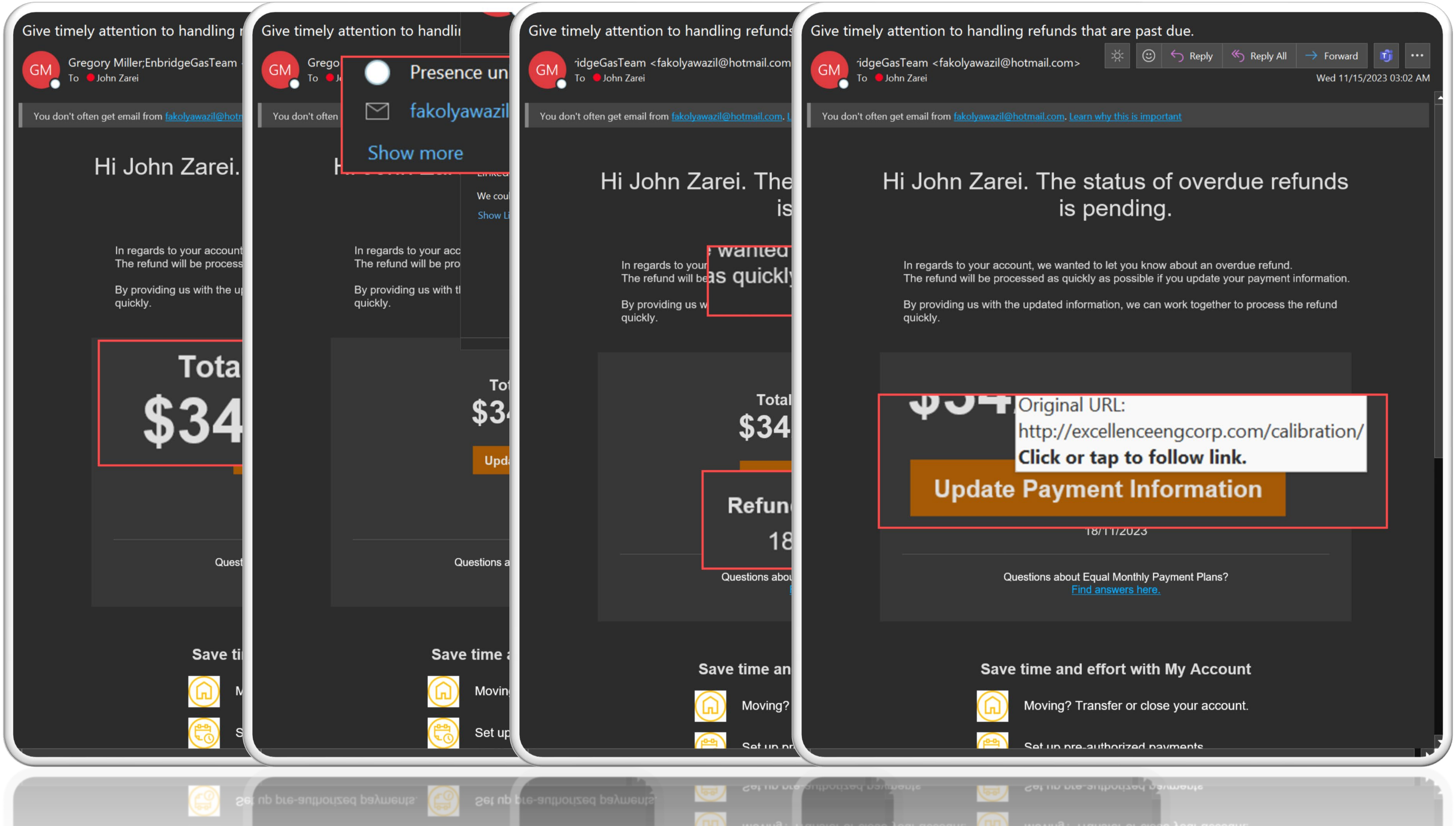
1. Asking for Personal Info.
2. Inconsistencies in Links
3. Unrealistic Threats
4. Generic Greetings
5. A Sense of Urgency
6. You're Asked to Send Money
7. Too Good to be True
8. Poor Spelling & Grammer
9. **Suspicious Attachments**
10. From Government Agency

Attachments aren't always malicious, but use extreme caution whenever you receive them unexpectedly.

10 Common Traits of Phishing

1. Asking for Personal Info.
2. Inconsistencies in Links
3. Unrealistic Threats
4. Generic Greetings
5. A Sense of Urgency
6. You're Asked to Send Money
7. Too Good to be True
8. Poor Spelling & Grammer
9. Suspicious Attachments
10. **From Government Agency**

In almost every case, **government agencies don't use email to communicate anything of consequence**. The CRA/IRS, for example, will never email you about your taxes or payment.

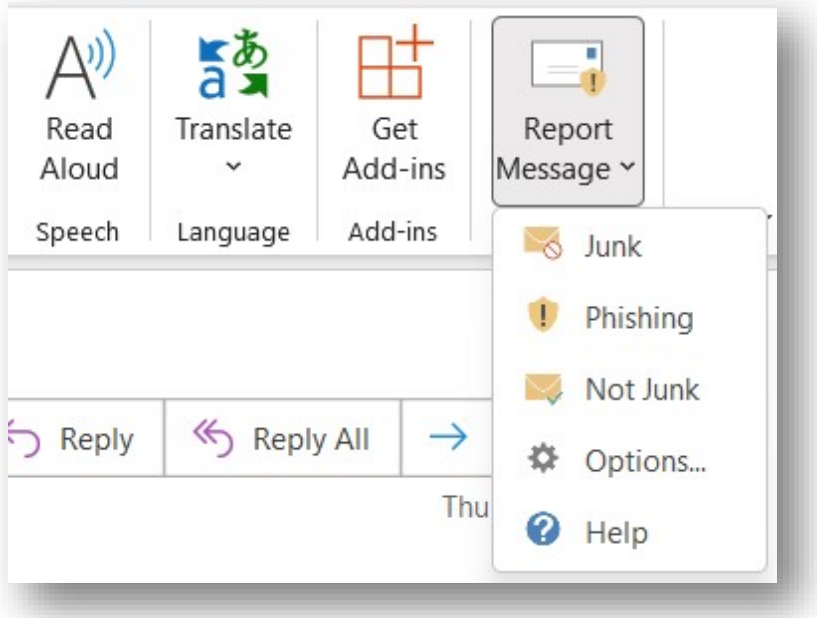

Give timely attention to handling refunds that are past due.
GM
ridgeGasTeam <fakolyawazil@hotmail.com>
To John Zarei
Reply
Reply All
Forward
Wed 11/15/2023 03:02 AM
You don't often get email from fakolyawazil@hotmail.com. Learn why this is important
Hi John Zarei. The status of overdue refunds is pending.
In regards to your account, we wanted to let you know about an overdue refund.
The refund will be processed as quickly as possible if you update your payment information.
By providing us with the updated information, we can work together to process the refund quickly.
Original URL:
http://excellenceengcorp.com/calibration/
Click or tap to follow link.
Update Payment Information
18/11/2023
Questions about Equal Monthly Payment Plans?
Find answers here.
Save time and effort with My Account
Moving? Transfer or close your account.
Gregory Miller;EnbridgeGasTeam
Presence un
fakolyawazil
Show more
Total
$34
Refun
18

Use the Outlook Report Message

Report suspicious messages to Microsoft as well as manage how your Microsoft 365 email account treats these messages.

Messages that your Microsoft 365 email account marks as junk are automatically moved to your Junk Email folder.

If you choose Junk, Phishing, or Not Junk, you'll have the option to send a copy of the message to Microsoft, along with your classification of the message.



Securing the sign-in process

One of the most important ways to ensure the safety of your online accounts is to keep your sign-in process secure.

Create strong passwords

Keep passwords secure

Create strong passwords

Hackers don't break in; they sign-in. If you use passwords as part of your sign-in process, you'll need to make sure they are as strong as possible.

Strong passwords are:

- At least 12 characters long (but 14 or more is better)
- A combination of uppercase letters, lowercase letters, numbers, and symbols
- Not a word that can be found in a dictionary or the name of a person, character, product, or organization
- Significantly different from your previous passwords
- Easy for you to remember but difficult for others to guess

kaspersky password checker

EN FAQ

9ap$0tHATHe

Time for a password change!

- Your password is easily crackable.
  - ⚠ Frequently used words
- Your password does not appear in any databases of leaked passwords

This password can be cracked faster than the time it takes to get back from a short walk

kaspersky password checker

EN FAQ

9ap$0tHATHe1

Nice password!

- Your password is hack-resistant.
- Your password does not appear in any databases of leaked passwords

Your password will be bruteforced with an average home computer in approximately...

2 centuries

kaspersky password checker

EN FAQ

9ap$0tHATHe1!

Nice password!

- Your password is hack-resistant.
- Your password does not appear in any databases of leaked passwords

Your password will be bruteforced with an average home computer in approximately...

10 centuries

kaspersky password checker

EN FAQ

Mydogisbobby

Time for a password change!

- Your password is easily crackable.
  - ⚠ Frequently used words
- Your password does not appear in any databases of leaked passwords

This password can be cracked faster than the time it takes to get back from a short walk

kaspersky password checker

EN FAQ

Mydogisbobbyfromtoronto

Nice password!

- Your password is hack-resistant.
- Your password does not appear in any databases of leaked passwords

Your password will be bruteforced with an average home computer in approximately...

3225 centuries

kaspersky password checker

EN FAQ

Mydogisbobbyfromtoronto2023!!

Nice password!

- Your password is hack-resistant.
- Your password does not appear in any databases of leaked passwords

Your password will be bruteforced with an average home computer in approximately...

10000+ centuries

Keep passwords secure

Once you've created strong passwords that hackers can't crack, you must keep them secure. If they can't break your passwords, criminals will try to trick you into revealing them.

To keep your passwords as safe as possible, follow these guidelines:

- ✓Don't share a password with anyone—not even a friend or family member
- ✓Never send a password by email, instant message, or any other means of communication that is not reliably secure
- ✓Never re-use the same password—all your passwords should be unique
- ✓Update your passwords frequently
- ✓Always access websites using trusted links
- ✓Don't hesitate to change passwords immediately on accounts you suspect may have been compromised

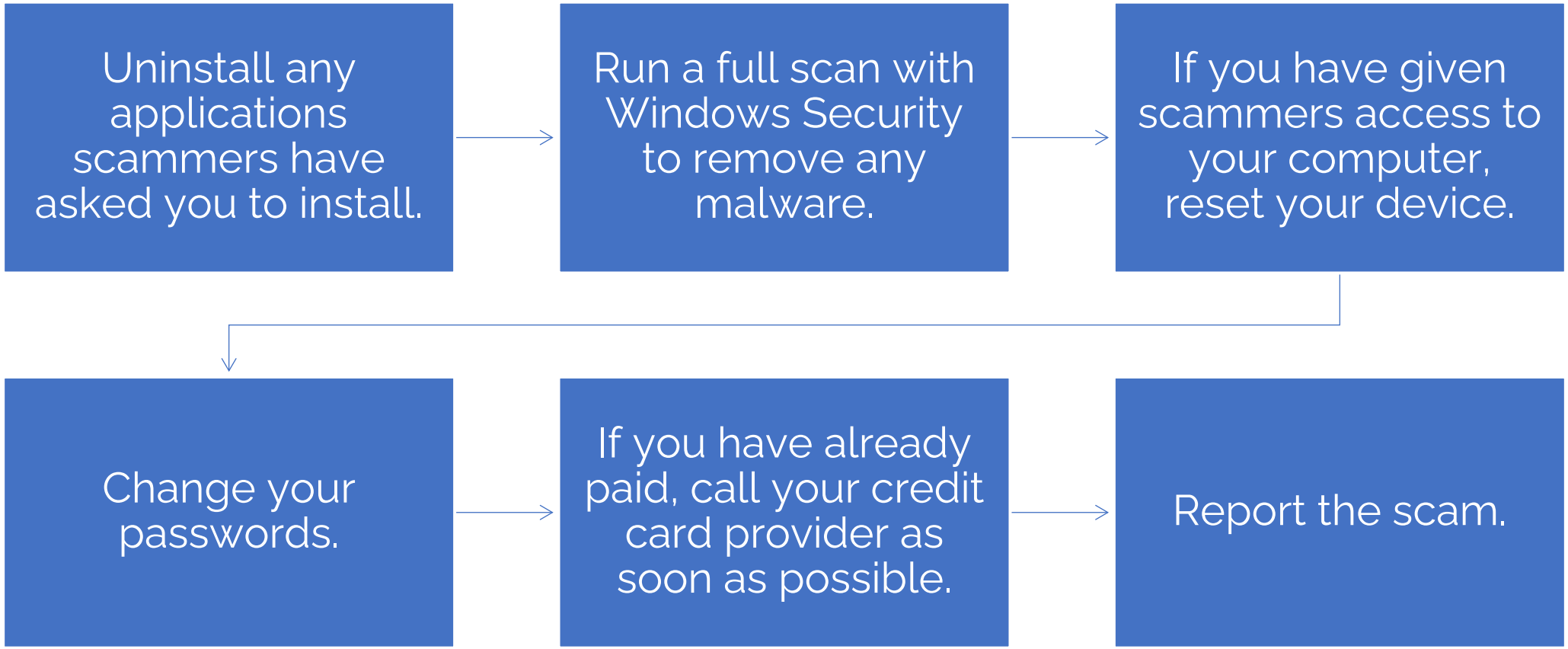
Tech support scam

In a tech support scam, criminals trick you into believing that you require a repair for your software or device. Some scammers may try to charge a fee to “fix” the nonexistent problem, and others will attempt to steal your personal or financial data or even try to access your network in order to deploy ransomware.

5 tell-tale signs of a Tech support scam

- You get an unexpected call from someone claiming to be tech support (Be aware! Some scammers have tools to generate fake Caller IDs).
- You get an error message asking you to call a number urgently.
- Your tech support contact asks you to pay them to fix your “problems” with cryptocurrency or gift cards.
- Your support technician asks you to download software from an email or third-party website.
- Tech support asks you for your password or other private, sensitive data.

What to do if you think you're in the middle of an attempted tech support scam?



Working more securely while travelling

There's a lot of good advice out there about picking a space that's ergonomically comfortable, and where you can minimize distraction, **but there are some security considerations as well**.

Working more securely while travelling

Pick a space that's private. Select a place where people can't "shoulder surf"; look over your shoulder at what's on your screen.

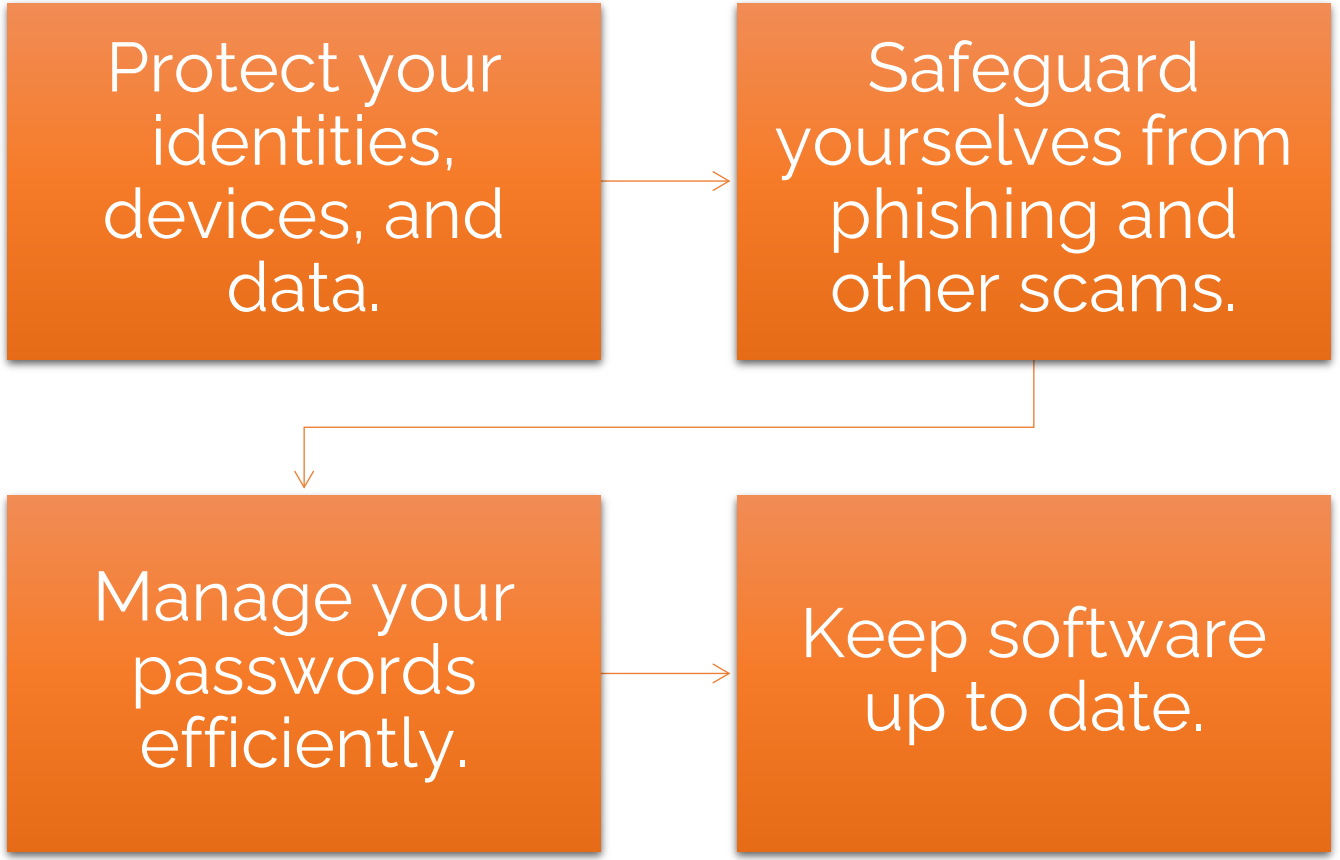
If you're having conference calls or video meetings, be aware of whether other people might be able to eavesdrop, even inadvertently. Even if (sometimes especially if) you're wearing headphones. Other people may still be able to hear your voice when you speak.

Don't allow others to use your work devices. If you have to walk away from your device, lock your device to prevent others from seeing what you're working on. Press Windows logo key + L on a Windows device, to quickly lock your screen.

Only use encrypted Wi-Fi for business. Wi-Fi encrypted with WPA-2 is more secure than Wi-Fi that is open for all to access.

Avoid using free charging stations in airports, hotels or shopping centers. Bad actors have figured out ways to use public USB ports to introduce malware and monitoring software onto devices. Carry your own charger and USB cord and use an electrical outlet instead.

Next Steps: Empower everyone to be a cybersecurity champion



Resources

- 1ty.me - One Time Self Destructing Links For Sharing Sensitive Information
- Norton Password Generator
- Password Check | Kaspersky
- Have I Been Pwned: Check if your email has been compromised in a data breach

Questions?