CYBERSECURITY 101

TIPS FOR KEEPING YOUR ONLINE ACCOUNTS SAFE

DISTRIBUTED OCTOBER 2021

Dear Rhode Island Voter,

October is Cybersecurity Awareness Month. As your Secretary of State, it is my responsibility to make sure you are able to exercise your right to vote safely and securely. I'm also keenly aware of common pitfalls that leave voters vulnerable to cybercrimes and identity theft. Seniors are more often targeted for cybercrimes as they usually have better credit and more wealth.

Nellie M. Gorbea
Secretary of State

I encourage you to read this handout with best practices to keep your email and online accounts safe as well as tips for identifying scams. I've also included information about how you can safely and securely check your voter registration information to make sure you are voter ready for every election.

Please don't hesitate to contact me by emailing SecretaryGorbea@sos.ri.gov or calling 401.222.2357 if you have questions or concerns.

SPOTTING COMMON CYBER SCAMS

Cybercriminals know how to pose as friends or family members, banks, charities, and seemingly legitimate online vendors to steal your information and gain access to your financial and personal accounts. Below are some common scams used against older Rhode Islanders to gain access to financial accounts. If you have fallen victim to a scam, report it to your local authorities immediately!

Family Emergency: Criminals use social media to gather information about your loved ones. Then they contact you about a loved one who needs emergency financial help either because of an injury "while traveling" or trouble with the law.

Government Impersonation: Criminals impersonate government employees. They may threaten action unless you agree to provide payments or urge you to click a hyperlink for important benefits information.

Tech Support: Criminals pose as technology support representatives and offer to fix non-existent computer issues.

Financial Services: Criminals target potential victims using illegitimate credentials from legitimate services, such as banks, mortgage or other credit companies.

FREQUENTLY USED TERMS

Malware: Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer. Typically installed when a user clicks on a maliciou**s link or downloads a malicious atta**chment sent in an email.

Phishing: When cybercriminals send an email or create a website posing as a legitimate business/organization to acquire sensitive information such as financial account passwords. Content usually creates a sense of urgency for the user to open an attachment or click on a link, immediately leaving the computer vulnerable.

Ransomware: A form of malware that deliberately prevents the user from accessing their computer files until a "ransom" is paid.

Smishing: When cybercriminals send text messages posing as a reputable company/organization in order to prompt individuals to reveal personal information, such as passwords or credit card numbers.

Spyware: A type of malware that spies on user activity including password keystrokes and financial accounts.

Virus: A type of malware aimed to corrupt, erase or modify information on a computer.

Vishing: When cybercriminals pose as a legitimate business or organization over the phone to acquire sensitive information such as social security numbers. Like phishing emails, the criminal will create a sense of urgency or an emergency that needs to be immediately resolved.

10 TIPS TO AVOID AND STOP CYBER SCAMS

1. Resist the scammer's urge for you to act quickly. Scammers are very skilled at manipulating emotions and will fabricate an emergency to persuade you to act without thinking.

2. Never send money or personally identifiable information to unverified people or businesses.

3. Be suspicious about anyone who demands gift cards as payment.

4. Most businesses or organizations don't ask for your personal information over email or text message. Before clicking on a link or acting on an urgent request, search for information about the company or government agency making the offer.

5. Beware of "free" gifts or prizes. If something appears too good to be true, then it probably is.

6. Be cautious what you download. Never open email attachments from someone you don't know and be wary of attachments included in email forwarded from friends.

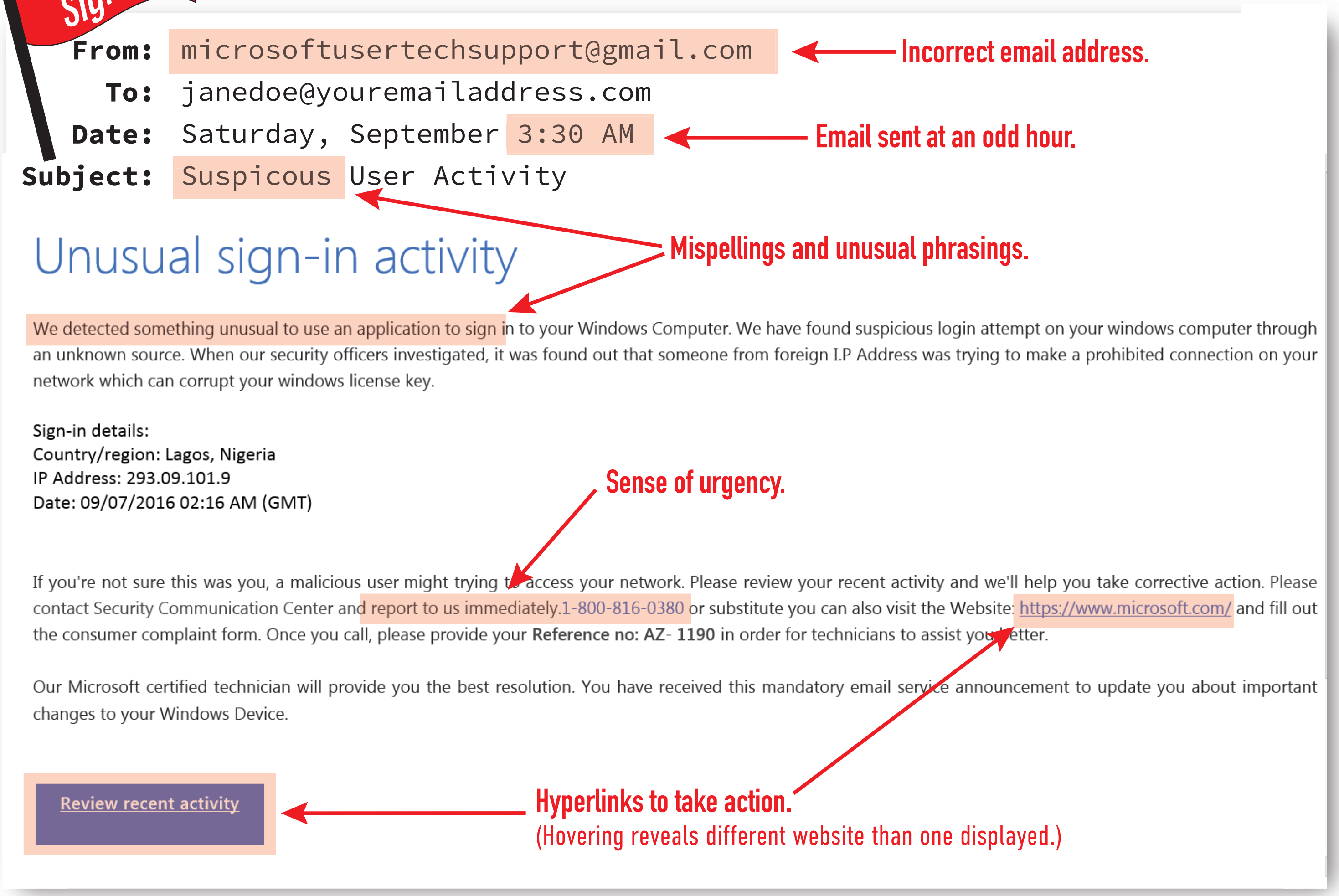
7. Disconnect from the internet and shut down your device if you see unusual pop-ups or get a locked screen.

8. Use reputable antivirus software and make sure you regularly update them.

9. Make sure your passwords are strong and different across different sites. *(See "Creating Strong Passwords" on page 3.)*

10. Be careful what you share on social media! *(See "Social Media Best Practices" on page 3.)*

RECOGNIZE THE RED FLAGS OF PHISHING EMAILS



From: microsoftusertechsupport@gmail.com
To: janedoe@youremailaddress.com
Date: Saturday, September 3:30 AM
Subject: Suspicous User Activity

Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ- 1190** in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

Incorrect email address.

Email sent at an odd hour.

Mispellings and unusual phrasings.

Sense of urgency.

Hyperlinks to take action.
(Hovering reveals different website than one displayed.)

Email image courtesy phishing.org.

SOCIAL MEDIA BEST PRACTICES

Social media is a tool used by cybercriminals to gather information about you and your loved ones. Here are some tips to be more social media savvy!

- Check your privacy settings and limit the amount of personal information you share publicly.
- Never share dates or information about trips before or while you are traveling.
- Only accept friend requests from individuals you know or trust.
- Avoid fun quizzes and polls. Scammers use them to identify answers to common online security questions such as your first pet, your first car or where/when you went to high school.

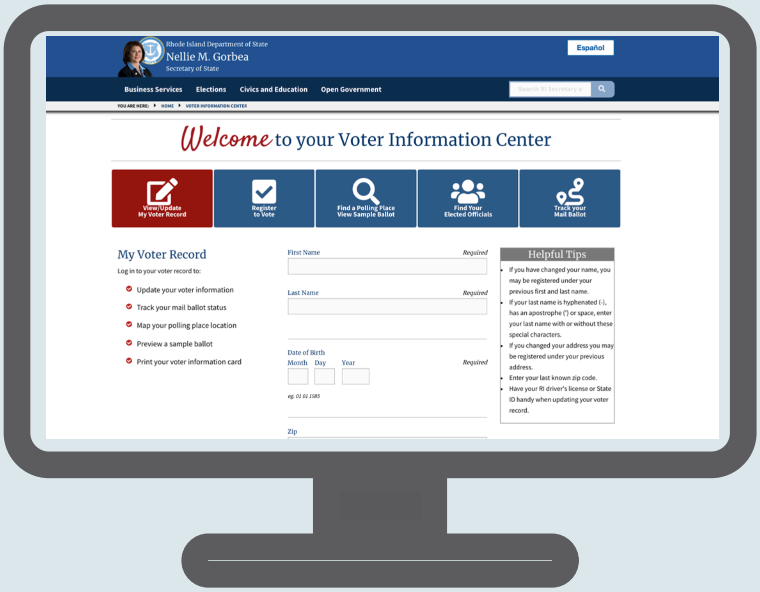
CREATING STRONG PASSWORDS

Strong passwords help keep your online accounts safe and secure. Here are some tips for creating strong passwords.

- Choose passwords that mean something to you and you only. ***Do not include commonly known information such as birth dates, anniversary dates or maiden/middle names.***
- Avoid words. Instead think of a favorite song lyric and use the first letter of each word as your password. Or replace some letters with numbers and special characters. Password generators can help!
- Do not use the same password for multiple online accounts. Use a password manager to keep your passwords securely organized.

BE VOTER READY!

It is important to make sure your voter registration information is always accurate and up to date! Here are the steps to quickly and securely check your voter registration information online:


Rhode Island Department of State
Nellie M. Gorbea
Secretary of State
Español
Business Services
Elections
Civics and Education
Open Government
Search RI Secretary o
YOU ARE HERE: HOME VOTER INFORMATION CENTER
View/Update My Voter Record
Register to Vote
Find a Polling Place View Sample Ballot
Find Your Elected Officials
Track your Mail Ballot

Welcome to your Voter Information Center

My Voter Record

Log in to your voter record to:

- Update your voter information
- Track your mail ballot status
- Map your polling place location
- Preview a sample ballot
- Print your voter information card

First Name *Required*

Last Name *Required*

Date of Birth *Required*

Month Day Year

eg. 01 01 1985

Zip

Helpful Tips

- If you have changed your name, you may be registered under your previous first and last name.
- If your last name is hyphenated (-), has an apostrophe (') or space, enter your last name with or without these special characters.
- If you changed your address you may be registered under your previous address.
- Enter your last known zip code.
- Have your RI driver's license or State ID handy when updating your voter record.

1 Go to vote.ri.gov.

2 Click “View/Update My Voter Record.”

3 Fill in the required fields and hit “Continue.”

4 You will be brought to your Voter Information page where you can confirm that your address and party affiliation are accurate. If it is accurate, you may close your browser window.

5 To update your address or party affiliation, simply click “Edit my voter record.” *You will need a valid RI Driver’s License or State ID to log in and make edits to your voter record*. Follow the steps to update your voter information.

Alternatively, you can click on the link to download and fill out a paper voter registration form.

BE VOTER SMART - HELP STOP DISINFORMATION

False information is shared on social media both mistakenly (known as **misinformation**) and intentionally (known as **disinformation**). Unfortunately ALL false information shared on social media leads to voter confusion and can result in voters not trusting the integrity of elections. You can help stop the spread of false information by asking yourself the following questions:

- Are multiple news outlets reporting the same story or is it one lesser known media site?
- Is the headline or image outrageous in an effort to get clicks? What’s the whole story?
- Is the author credible? Do they have a long history covering the topic? Are they known for writing news, satire, or personal opinion pieces?
- Are there supporting sources included in the story?
- Are your own beliefs affecting your judgment?

When in doubt, check with state or your local elections officials with any questions about elections in Rhode Island.

Rhode Island Department of State | Elections Division
148 West River Street, Providence, 02904
401.222.2340 | elections@sos.ri.gov