THE BASICS OF ONLINE SECURITY (November 2021)

BY: Parker Gibson, Systems and Security Administrator.

Staying safe online is a major concern in today's digital market. While it may seem like online finances and shopping are the most obvious targets for a cyber-attack, it is important to remember that hackers constantly probe much more than just those. Any machine connected to the public internet receives an endless stream of exploit attempts. This is why it is so important to never plug a computer directly into your modem. You should always have your home computers connected to a router, which shields them from direct access from the internet.

Modern technology only works because millions of systems all over the internet must be able to securely communicate with each other. Take Netflix for example, you can sign into Netflix using your Facebook account, which uses a portal connected to Google's reCAPTCHA service to protect against bot attacks so can pay your bill using your bank debit card. (reCAPTCHA is the "I'm not a robot" prompt that sometimes asks you to identify parts of images with certain characteristics. CAPTCHA is the old model which asks you to verify certain blurry or unclear words). Just that simple activity securely reaches out to at least four service providers. Unfortunately, this is the norm, and as we learned in 2017 with the Equifax breach, 147 million companies that they had never even volunteered their information to, had that information, and were compromised.

This should not make you overly paranoid. Most of the time these interactions go off without a hitch. The unfortunate reality, however, is that businesses MUST have an online presence now, and while a security engineer needs to protect against countless security vulnerabilities when building and linking systems, a hacker only needs to find a single vulnerability to start his attack.

The truth is, it is almost inevitable your sensitive personal information will be exposed at some point. Even if you do not use the internet at all, your subscription to Time magazine or your utility provider have your information stored on systems which are connected to the internet.

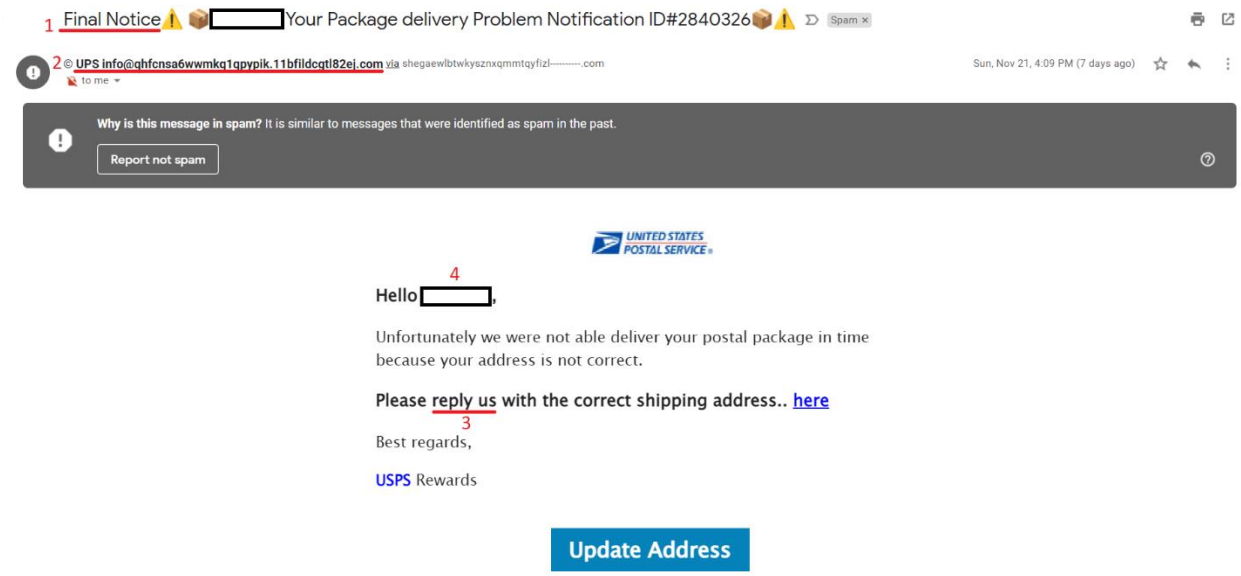
There are some important steps that will help to keep you safe. These will be expanded on later, but boiled down these steps are:

1. **Phishy Emails**: Never click on a link or download attachments from emails you do not know.
2. **Strong Passwords**: Choose strong passwords. Despite what you have been told, it is better to have longer but easier to remember pass*phrases*, instead of complex, hard to remember passwords. Avoid using commonly used passwords like "password" or "password123". Do not reuse passwords across websites.
3. **Your Debit Card Has a PIN for a Reason**: Use multi-factor authentication on any site that offers it. If they have the option to alert you to new login activity, enable that too. Always sign up using an email address that you have access to and monitor.
4. **That Little Padlock in Your Browser's Address Bar**: The little padlock tells you the website is secure. Do not use websites that are not verified as secure in your browser. All modern browsers will alert you when the security certificate of a website cannot be verified. Remember, just because a site is verified as secure, doesn't mean it's not malicious, but a trusted site that has a certificate error is a red flag that someone may be trying to spoof the site.
5. **Be Careful with Your Selfies:** Use caution when posting on social media. Be aware of details that bad guys can use, such as posting vacation pictures while still out of town or personal information such as mother's maiden name or names of pets.

6. **Your Computer Needs Updates**: Computer updates might be frustrating, but they are a vital tool to keeping your system secure. Your devices will install updates from the manufacturer automatically but be wary of downloading products that claim to manage updates for you, as they are often vectors for attack.

1. Phishy Emails

By far, the most common way people have their data compromised, is through email scams. The stereotype of a hacker is that they are constantly exploiting systems with complex tech and tools, but the most common way they succeed, is through what are known as "phishing emails." A phishing email is an attempt to trick the person reading the email into taking action that would expose their information. Below is an example of a typical phishing email, with some of the signs it is suspicious or "phishy" underlined in red:



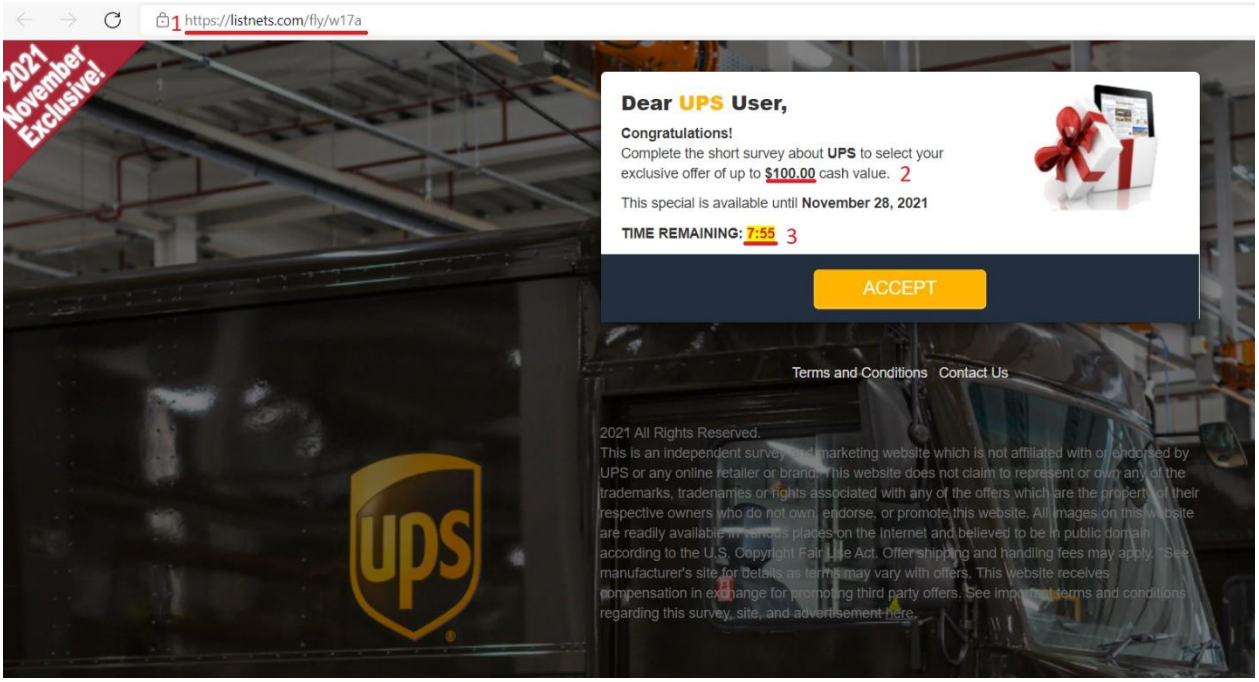
1. These emails commonly use a sense of urgency as a tactic to get people to click on a link in the email.
2. The display name of the email address is "UPS Info." While this name seems legitimate (even though it should say USPS instead of UPS), you can see the email domain is "@qhfcnsa6wwmkq1qpypik.11bfildcgtl82ej.com." This is most certainly not an email from USPS. Be careful when reviewing the email domain, as some phishing emails do a much better job than this one and may send from a domain such as "US-PS.com", which certainly seems less suspicious, but is not the correct domain.
3. Grammatical errors are common red flags in these emails. Keep an eye out and be cautious.
4. I have censored the name used in the email for my privacy, but it simply read as the first part of my email address. This is a red flag that my email was exposed somewhere, but they do not have a name associated with it. This is a very common red flag.
5. In this instance, my email provider, Gmail, has identified this email as spam based on other users reporting it. This is a common feature of email providers nowadays. Always pay attention to alerts such as these. Although sometimes legitimate emails may be marked as spam, you should always verify every email before clicking anything.

Additionally, when hovering over the “Update Address” link in the email, I can see in the bottom left of my browser the URL that it will take me to:

https://storage.googleapis.com/teampass/bombaaa/hope.html#2097211pj5388670lt557756506Jv688gi24eRr141554yg

Again, this URL is certainly not a USPS website.

And lastly, if I click the link I notice I am taken through a handful of redirects to different sites (by watching the navigation bar of my browser), before finally landing on the following page:

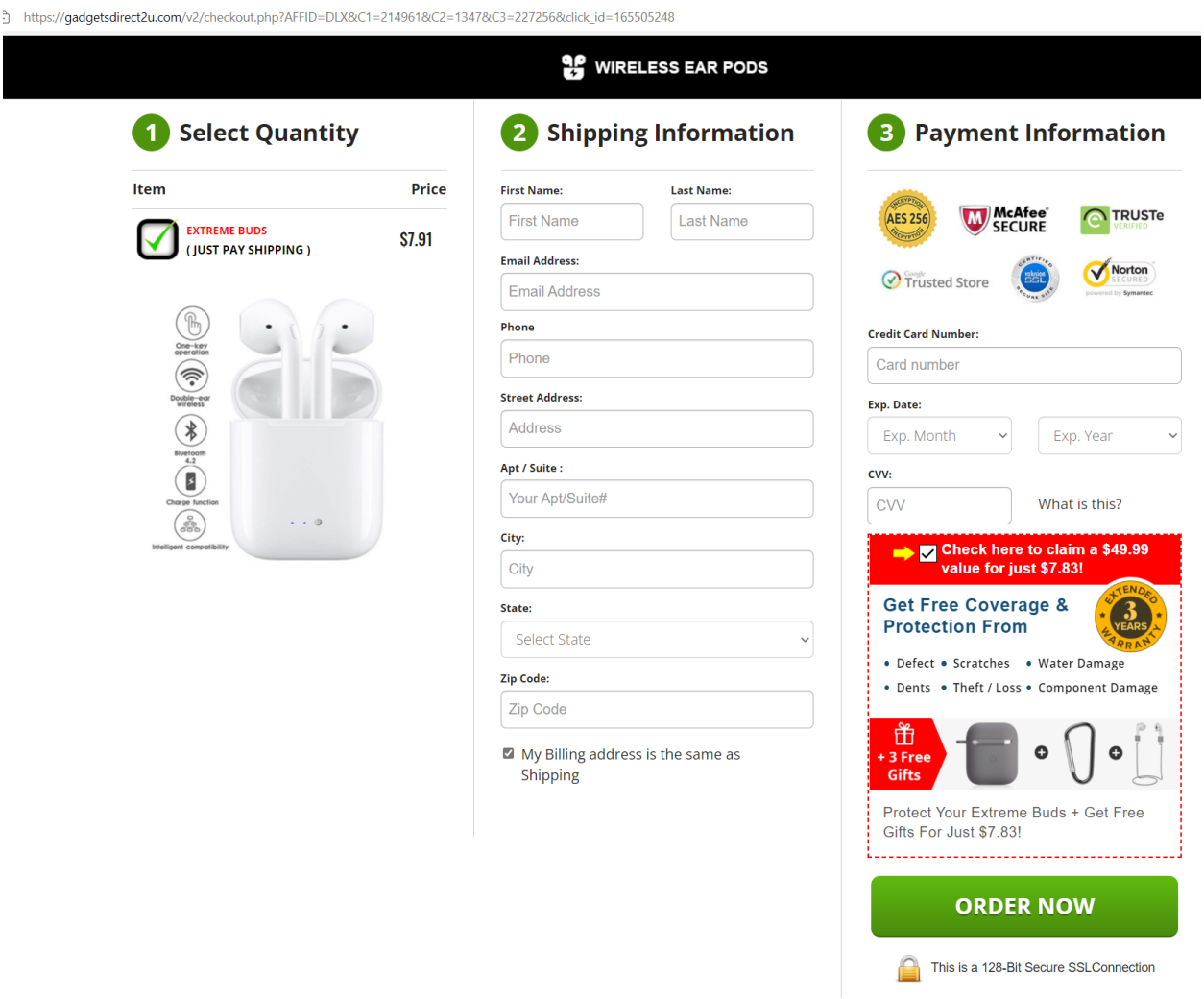


This is a poorly executed phishing email, which makes it a pretty typical example. Most phishing emails will have a number of red flags like these. I am taken to a page that looks like it could be legitimate, except the email I got had the USPS branding on it, and I was taken to a UPS branded site.

1. The URL is not a USPS URL, or a UPS URL for that matter.
2. I have an incentive to take the survey.
3. Another sense of urgency pushing me to finish the task quickly.

Furthermore, the email said I had a package that was not able to be delivered because my address was incorrect. I am not sure why I am being asked to take a survey. And again, we see a non-specific greeting.

After I fill out some vague questions about how satisfied I am with my UPS service, I am finally taken to the following page where I can enter all my shipping information and credit card number:



While this is a pretty typical approach to try and steal my credit card number, make sure you are on the lookout for more targeted attacks. For example, an email to your work address from the help desk or IT department, with your company logo on it, prompting you to confirm your password. When in doubt, always use a known good contact method to confirm the email such as a phone number or email from the correct URL (not the one linked to in the email) or contact information from a billing statement or invoice.

2. Strong Passwords

The attacker in the previous example had my email address, so they know my account (and possibly the username I use to log into my bank, Amazon, Netflix, Twitter, etc. if the service uses email address as username) but they don't know my password. It is safe to assume my email address is on a number of nefarious websites, where lists of known email addresses are posted for anyone to review or purchase.

If I have a weak password on any account associated with this email, it could make it much easier for an attacker to gain access. What is even more dangerous, is if I have a weak password on the email account itself. If an attacker gets into the email associated with my Amazon account for example, they may not be able to log into my Amazon account, but they can probably reset the password to that account because they have access to my email.

There are a number of ways hackers try to determine what the password to an account is. Here are some of the most common approaches:

1. **Brute Force Attacks**: An attacker sets up a program to automatically attempt to log into an account using sequentially generated passwords. These can be based off an algorithm, e.g. “aaaaaaaa”, “aaaaaaab”, “aaaaaaac”… “aaaaaaaz”, “aaaaaaba”, etc. but generally they will start with common passwords and variants before proceeding to a strictly algorithmic attack, e.g. “password1”, “password2”, “password3”, etc.

   As you can probably see, a password that is only 5 characters long, or is based off a common password or variant, will take less time to break with a brute force attack than a longer password.

2. **Dictionary Attacks**: Using the same technique as above, an attacker will try random words from a dictionary, and combinations of those words to try and guess a password.

   As you can probably see here, a password which is just a single dictionary word would be easily vulnerable to this attack.

3. **Password Spraying Attacks**: This type of attack uses the same automated approach as the previous two, but instead it uses huge lists of known passwords that have been compromised to see if any of them match your account.

   This is why reusing passwords across multiple accounts is a risk. If one of them gets compromised, even if you use a different account name on another website, the password could be discovered through this sort of an attack.

The last point I want to make here, is the traditional way we have been taught to create secure passwords is wrong. Traditionally, we have been told to use a mix of capital letters, lower case letters, numbers, and symbols to construct a password with no dictionary words in them. This makes the password incredibly hard for people to remember and doesn’t really defend well against most attack types. If you feel the need to write down a password, NEVER store the password in an easy to access location. Common locations are on sticky notes on the computer screen or under the keyboard or mouse pad. The better option is to use a secure password storage service such as the Keepass application, or the LastPass.com site.

The new standard, set by the National Institute of Science and Technology (NIST) in 2017, recommends people use passphrases in lieu of passwords. Passphrases are just that, a phrase you use as a password. This means it is easy for a human to remember, and hard for a computer to guess because they are so long. So, instead of using “ZD$&T53&K%-KbYuH”, you can use “Don’tYouStepOnMyBlueSuedeShoes”.

(The official NIST document can be found at the following URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf)

3. Your Debit Card Has a PIN for a Reason

Multi-factor authentication (MFA) is becoming commonplace, and for good reason. Traditionally, we relied solely on username and password to validate users, but we are continually seeing additional verification factors added to services. Many banks now require you to enter an SMS (text message) code

when logging into their site for the first time on a new computer. This is an example of MFA. MFA is defined as requiring at least two of the following three:

1. **Something you have:** Most commonly your phone to get the text message or check an app, or a security key with an encryption certificate on it (like a keycard).
2. **Something you know:** Generally, your username and password, but it can also be answers to security questions like your mother's maiden name, the street where you grew up, or your childhood best friend's name.
   NOTE: This is why it's important not to use things like your pet's name or your child's birthday as a password, as these things can be discovered by an attacker targeting you specifically simply by doing some research online and looking at Facebook, public records, obituaries, etc.
3. **Something you are:** This is generally a biometric. Because biometric technology (such as face recognition and fingerprint readers in phones) has become more reliable and affordable, these factors are becoming more common.

This means if a hacker had a good username and password for your account, but that account required MFA, they would be unable to log in without your second factor such as your fingerprint or your phone. This is why debit cards use PIN codes, someone would need to have your card (something you have), as well as the PIN (something you know) in order to use it. This has protected me personally. One of my accounts (one with a credit card linked to it) was compromised, and I got a number of alerts from the site letting me know there was an unsuccessful login to that account, so I was able to log in with MFA and change the password. If I had used a fake email to sign up for that account, I would not have known it had been compromised. If I had not had MFA setup, the account would have likely been used to make a number of purchases I didn't want.

4. That Little Padlock in Your Browser's Address Bar

You have probably heard that logging into your accounts from a coffee shop is a potential vector of attack. While this is technically true, the odds are extremely low an attacker would be able to get that information if you ensure you are always connected to a trusted site. This trust is verified through what is known as a "certificate authority" (CA). There are only a handful of CAs that dominate the market, and they create the trust between your browser and the site you are visiting.

This all works through encryption. I won't get into how encryption works here, but essentially encryption allows information to be sent securely, because it requires a private key to decrypt. A website has two certificates, a public certificate (public key), which the browser uses to encrypt data being sent, and a private certificate (private key), which allows the site to decrypt the data it receives from your browser. This method of encryption is what is known as asymmetrical encryption. Meaning that since the public key is available for anyone to see and use to encrypt, the same key cannot be used to decrypt that data. If someone intercepts the data being sent, without the private key, they have no hope of decrypting it. Even through a brute force style attack, with modern encryption methods, and the most sophisticated hardware, it would take more than 100x the age of planet earth to break it. Traffic is encrypted when a browser connects to a website via https:// rather than http:// on the URL in the address bar.

All modern websites use this encryption (known as SSL encryption), and that is what the padlock on your browser indicates. A CA (like GoDaddy) issues certificates to websites that are used to encrypt all traffic. These certificates can be validated against the CA by the browser, and if there is a mismatch, the browser will warn you that it cannot verify the certificate.

Furthermore, even if someone took the certificate that Amazon uses, and spoofed the domain in a coffee shop, if the browser is using an https (SSL) connection, they could not actually decrypt any of the data you sent to their spoofed site.

The certificate includes information about the site, including the domain, which is why you should always double check the domain you navigated to is the domain you intended. For example, with the UPS phishing email above, the browser trusted the site, because the domain matched the certificate that was purchased, but the site was definitely not trustworthy. This means when you are making online purchases, if you verify you are using an SSL connection, you are safe… as long as the site owner is trustworthy.

This is where services like PayPal come in. They function as a trusted broker for your transactions online. If you have the option to pay with PayPal, they ensure your credit card information is never exposed to the site owner. They simply broker the transaction. So, even if the site owner is not trustworthy and never ships the item, they have absolutely no way to charge your credit card again.

5. Be Careful With Your Selfies

Social media is everywhere, and it is important to use it safely. Many people post details on social media that can be used by criminals for nefarious purposes. For example, people will post vacation pictures online while they are on vacation. Anyone with bad intentions could use this information to discover that you are out of town, and your house is unoccupied.

Additionally, when sharing pictures (for example, if you start a blog and upload photos), be aware these pictures contain more information than what is immediately visible. While it may not be a good idea to post pictures of your expensive toys online, if you take the pictures with a phone, there is additional detail called metadata embedded in the photos. This information contains innocuous information like the type of camera used, and the time the picture was taken, but also often contains GPS coordinates of where the picture was taken. The following site allows you to read all the metadata of an image, and additionally, allows you to download a copy of the image with all metadata removed: https://www.verexif.com/en/

You should also use caution when posting personal details. For example, many sites use security profiles to reset passwords. Common questions are things like “What is your mother’s maiden name?”, “What street did you grow up on?”, “What was the make and model of the first car that you owned?”, or “What is the name of your first pet?”. These are details a diligent bad guy could discover by reviewing your social media and use to gain access to your accounts. In 2014, a massive leak of lewd celebrity photos was distributed online. The source of the photos was deemed to be iCloud backups, which were accessed by researching the answers to the celebrity security questions.

6. Your Computer Needs Updates

Another important thing to consider is computer updates. As exploits are discovered, and used, software manufactures become aware of them and fix (patch) them. These patches are part of what you get when you update your computer. Keeping your devices such as your computer, phone, router, game console, and even some cars updated is important to staying safe. It is never necessary to use a search engine to search for updates. Updates should only be downloaded from the manufacturer website, or by clicking the update prompt on the device (make sure it is not a web browser with a fake prompt). Never download “updates” from any site other than the manufacturer’s site. This is an extremely common way malware is distributed.

Lastly, there are resources to help you determine if your accounts have been compromised. The following site allows you to enter a username or phone number, and see if any credentials linked to that account have been posted on sites commonly used by bad guys to distribute such information: https://haveibeenpwned.com/

At the end of the day, it is safe to assume at least some of your accounts have been compromised. Make sure to keep an eye on your credit score, and bank statements, as well as your email inbox for any suspicious activity. Make sure you set up MFA on any accounts that support it and resist the urge to reuse passwords across sites. Unfortunately, in our modern economy, it is ultimately impossible to guarantee personal information is not exposed online. You should take measures to ensure that your accounts are protected and maintain a diligent watch for signs of unexpected activity.