Viridis Graduate Institute

Ecopsychology and Environmental Humanities

Cyber Security Awareness Training

Viridis Graduate Institute Cyber Awareness Policy

Students, Faculty, and Staff at Viridis Graduate Institute

☐ I AGREE to adhere to the following Viridis Graduate Institute Cyber Technology Policy and take all precautions to protect personal and Institutional information.

☐ Students, faculty, and staff are required to read and follow recommendation made in the Cyber Awareness Training and submit to VGI a signed copy of this Training.

☐ Students, faculty, and staff are required to communicate with each other, share non-personal data, or submit assignments using Viridis Gmail accounts.

☐ Faculty and students are required to communicate on all course and assignment questions, requesting information, or sharing ideas using Viridis Gmail accounts.

☐ Students, faculty, and staff are required to change VGI passwords periodically.

☐ Students are required to follow the Ethical Computer Use Institutional Policy found in the Catalog and Student Handbook.

Executive Staff only

☐ The Executive Team will encrypt all student educational records that are shared electronically, housed on personal computers or housed on VGI OCEANS.

☐ Viridis Graduate Institute does not share student data, information, or educational records with anyone. ONLY the student may reuest information pertaining to their educational records as stated in FERPA Laws in VGI Institutional Policies.

Cyber Awareness Training

We live in an amazing time where we are instantly connected to the entire world. We can communicate with anyone we want, anytime we want, anywhere we want. In addition, we now have access to just about any information we need at our fingertips.

However, with all these amazing advances come new risks. Now that the world is so interconnected, it has become much easier for cyber threats to attack and exploit our information. As a result, we are committed to an active information security program.

In the following training you will learn who is targeting you, how you will be attacked and why. In addition, we will teach you the steps you can take to protect yourself and our Institute.

You Are The Target

One of the most important things to understand is that you are a target. Many people mistakenly believe that cyber attackers only target our databases or web servers. In reality, they also target individuals like you. While these attackers use a variety of sophisticated tools, they have learned that the simplest way to hack into an Institute like ours is to target people like you.

Example:

Several months ago, a team of cyber attackers decided to target our Institute. We are not sure what their motivation was. Perhaps they wanted to steal our sensitive information, or make a political statement.

All we know is that they began searching our website several weeks ago, learning everything they could about us. This included who we are, how we operate and the identities of employees and staff. They then began to harvest employees' personal information from websites such as Facebook, YouTube, LinkedIn, Instagram and public forums.

Unfortunately, several people had posted too much information about themselves and the Institute. As a result, the attackers were able to build a complete picture of the Institute and learn details about key members of our staff. Armed with this information, they launched their attack.

Seven people at the Institute received emails that appeared to come from a package delivery service we commonly use. While these emails appeared to be legitimate, they were actually phishing emails created by the attackers. Each message contained an infected email attachment designed to bypass our anti-virus software and silently infect our computers.

Unfortunately, two of the targeted employees fell victim to the phishing emails by opening the attachments. The attackers then installed key-logging software on the computers, enabling them to capture all of the employees' keystrokes.

On one of the hacked computers, an employee was using a login and password they had shared with their coworkers. The attackers quickly harvested this information and were able to log into other systems throughout our Institute. Because the attackers were using stolen, legitimate passwords, our security team did not detect the attackers.

Over the next seven days the attackers scanned the hard drives of numerous compromised systems, stealing every document, spreadsheet and presentation they could find. They soon transferred over 150 Gigabytes of confidential information out of our Institute, including a key project we had been working on for over three months. Fortunately, an alert employee noticed several suspicious programs running on their computer and reported it. As a result, the attackers were finally detected and blocked from causing any more harm.

While this is ***only an example*** provided for illustrative purposes, it demonstrates why we have security policies and controls. They are carefully designed to protect you and Viridis Graduate Institute, while also ensuring that we are compliant with important standards and regulations. This is also why it is so important

that you understand and follow our security policies.

You may not realize it, but you are even under attack when you and your family connect to the Internet at home. To help protect yourself, your family and our Viridis Graduate Institute, always remember some core principles:

- Always be cautious and assume you are a target. You may not think you or your information has value, but it does.
- Attacks are a constant threat on the Internet. If something seems suspicious or too good to be true, it most likely is.

Social Engineering

How cyber attackers compromise our computers and steal our information: one of the main techniques they use is called social engineering, which is also known as the art of human manipulation. This is when attackers pretend to be someone or something you know or trust, such as your bank, a government organization, or even a friend or coworker.

They then leverage that trust to get what they want, often by simply asking for it.

EXAMPLE

You receive a phone call from someone claiming to be from a computer support company. They explain that your computer is behaving strangely, doing things like randomly scanning the Internet, and they believe it is infected. They tell you they have been tasked with investigating the issue and helping you secure your computer. They then use a variety of technical terms and take you through confusing steps to convince you that your computer is infected.

For example, they may ask you to find specific files on your computer and explain how to find them. When you locate these files, the caller will explain that they are a sign that your computer is infected. In reality, these files are just common files found on every computer.

Once they trick you into believing your computer is infected, they will pressure you into going to a website and buying their security software. However, the software they are selling is not really security software. It is actually an infected program that will give them total control of your computer. In the end, not only have they fooled you into infecting your computer, but you just paid them to do it.

Social engineering attacks like these are not limited to just phone calls. Attackers can leverage almost any technology to fool you, including email, instant messaging or text messages, and can even do it in person.

Common indicators of a social engineering attack include people asking for information they should not have access to, using a lot of confusing or technical terms or creating a sense of urgency. If you believe someone is attempting to trick or fool you, simply hang up the phone or ignore the email or report the email as spam.

Email and Messaging

Email is one of the most powerful weapons in the cyber attacker's arsenal, simply because so many people depend on it in their daily lives. With email, an attacker can easily pretend to be someone or something you trust, such as your friend or your bank. These attacks, often called phishing, work by tricking you into doing something seemingly harmless, like clicking on a link or opening an attachment.

For example, a phishing email pretending to be a well-known bank. The email is very professional looking, including the bank's logo. The email says there is a problem with your account and that if you do not update your account immediately, it will be deactivated. It then requires you to click on a link and log into a website.

If you click on this link you are taken to a website controlled by the cyber attacker, who silently hacks into your browser, infects your computer and takes control of it. Alternatively, attackers will send emails with infected attachments instead of links.

In addition to generic phishing attacks that can target anyone, attackers can utilize a more specialized attack called spear phishing. This is a highly targeted attack where only a few emails are sent to specific individuals within our Institute. These emails appear very realistic, often with a subject that is relevant to the victim's job or appear to come from individuals that the victim highly trusts.

Finally, there is messaging. Just like email, almost any type of messaging can be used for phishing attacks, such as those on Facebook, Skype, Twitter or your smartphone. Always be careful of messages, regardless of what technology you use.

In most cases, simply opening an email or reading a message is safe. For most attacks to work, you have to do something after reading the message, such as opening the attachment, clicking on the link or responding to the request for information. To protect yourself, keep the following in mind:

- Just because a message appears to come from a friend or someone you know does not mean that the message is safe. Cyber criminals may have infected their computer, hacked their account or spoofed the 'From' address. If you are suspicious about a message from someone you know, call the person to verify if they really sent it.

- Be suspicious of any email directed to "Dear Customer" or some other generic salutation.

- Be skeptical of any message that requires "immediate action," creates a sense of urgency or threatens to shut down your account.

- Before you click on a link, hover your mouse cursor over it. This will display the true destination of where it will take you. Confirm that the destination displayed matches the destination in the email and make sure it is going to the Viridis Graduate Institute's legitimate website. Even better, type the proper website address into your browser. For example, if you get an email from your bank asking you to update your bank account, type your bank's website into your browser, then log into the website directly. On a mobile device? No problem. Simply hold your finger down on the link and you should see the true destination in a pop-up window.

- Be careful with attachments and only open those you were expecting.

Always double check that you are emailing the correct person before sending one, especially when sending something sensitive.

Browsing

Cyber attackers have developed numerous techniques for attacking your browser. A common technique they use is to place tools designed to hack into your browser on websites that you might visit. The malicious tools then silently probe your browser and launch multiple attacks when you visit the sites.

If your browser or any of your plugins are outdated or vulnerable, your computer will most likely become infected. Unfortunately, there is no simple way to tell if a website is safe or not, so it is important you take some simple precautions.

- First, most browsers maintain a list of known malicious websites that intend to cause you harm. If you accidently visit one of these known websites, your browser will post a warning like you see here. If your browser warns you against visiting a website like this, do not connect to it.

- Always use the most current version of your browser and ensure it is up-to-date. This prevents attackers from exploiting known weaknesses and is one of the most effective ways to protect yourself.

- Do not install plugins or add-ons for your browser unless you absolutely need them and have prior approval. Plugins make it easier for attackers to hack your computer. If you do have plugins installed, make sure they are as up-to-date as your browser.

- Be sure your connection is encrypted whenever you connect to sensitive websites, such as online banking. Look for signs of encryption like the website address starting with HTTPS and a padlock icon in the status bar.

- Finally, always be sure to scan any files you download with anti-virus.

Social Networks

Social networking websites are one of the most exciting technologies on the Internet. What makes these sites so powerful is how easy it is to share with others and to watch and learn what others are doing. However, there are risks that come with these amazing capabilities that you need to be aware of.

First, be careful what information you post. People can use that information to steal your identity, guess your passwords or commit online fraud. Some websites, such as Facebook, offer privacy controls that allow you to control who can access what information. The problem with privacy controls is that they are complex, change often and do not always work as you expect.

The best way to protect yourself is to assume any information you post will eventually become public, regardless of the privacy controls you use. If you do not want your boss or family to find out about it, do not post it.

Also be careful of what others post about you. Your friends may be posting confidential information or personal photos of you. Ask your friends to be considerate of your privacy and track what they are posting about you. If they post anything you feel is inappropriate, ask them to remove the content or report it to the website's abuse department.

Cyber attackers may attempt to fool you on social networking sites, just like they do in email or instant messaging. A common attack on sites like Facebook or Twitter is for a criminal to hack into a person's account and post messages pretending to be that person.

For example, your friend may post that she was just mugged while traveling overseas and lost all of her money and documentation. Shee desperately needs help and asks if you or anyone else can transfer some money right away. The problem is that your friend was never mugged. In fact, she was never even traveling. Instead, someone hacked into your friend's Facebook account and posted the fake message pretending to be her.

Also be careful of 3rd party applications that integrate with social networking sites. They may be infected or attempt to access your personal information. When you stop using the 3rd party application, uninstall or disable its access to your social networking profile.

Finally, D O N O T not post any confidential information about Viridis Graduate Institute on any websites.

Mobile Device Security

Mobile devices, such as smartphones and tablets, have become incredibly powerful. These combinations of factors make mobile devices very useful, however it also can put you at great risk. To protect yourself, we recommend the following:

- Just like with your computer, install only apps that you need and make sure that you download them from trusted sources. Criminals can create apps that look real, but are actually malicious programs designed to quietly take control of your devices. In addition, do not install apps that request excessive permissions, such as the ability to silently send text messages or copy your address book.

- Just like with your computer, backup your mobile device on a regular basis. This way, if something happens to the device, your information is not lost.

- Make sure you update your mobile device and apps on a regular basis. Cyber attackers can more easily exploit your devices if you are running outdated software. If your mobile device is old and no longer supported, consider purchasing a new one that can support the latest version of the operating system and security updates.

- If you have security software installed, such as anti-virus or a firewall, then make sure they are enabled and updated with the latest version.

- Remember that many of the attacks you find in email can also happen via texting on your mobile device. For example, cyber criminals can text messages asking you to connect to malicious websites, download infected apps, or ask you for private information such as your bank account. If a text message seems suspicious or too good to be true, simply delete it.

- Be careful when using Wi-Fi. Many mobile devices will automatically connect to Wi-Fi networks without asking you, putting your device at risk. Disable Wi-Fi if you are not using it.

- Attackers can also take advantage of your Bluetooth capabilities. Just like Wi-Fi, disable Bluetooth

when you are not using it. It is also important to turn off Bluetooth discoverable mode features.

- Do not access or store work email or other data from our Viridis Graduate Institute on your mobile device. Protect your devices with a hard-to- guess password or PIN. If your device supports encryption, we recommend you use it. Also, consider enabling remote wiping if available. This means if your mobile device is lost or stolen, you can erase all your information remotely.

Passwords

Once someone knows your password, they can steal your identity or access all of your personal information. Let's learn what makes a good password and how to use them securely. There are two key points to good passwords:

- First, you want passwords that are hard to guess. This means - do not use simple passwords such as 123456, your pet's name or your birth date.

- Second, use passwords that are easy to remember. If you keep forgetting your passwords they are not very helpful.

The problem is cyber criminals have developed sophisticated programs that can guess, or brute force your passwords, and they are constantly getting better at it. This means they can break into your accounts if your passwords are not strong enough. To protect yourself, you want your password to be as long as possible. The longer your password is, the stronger it is. Instead of using just a single word as your password, use multiple words. This is called a passphrase. To make your passphrase even more secure, do the following:

- Use a number in your passphrase.
- Have at least one lower case and one upper case letter in your passphrase.
- Use a symbol in your passphrase.

Data Security

A great deal of our security focuses on keeping your devices secure. While this is important, understand that most attackers are not after your devices but the sensitive information that resides on them. Examples of sensitive information can include credit card numbers and personally identifiable information. As such, you should take the following steps when handling sensitive information:

- Always understand the sensitivity of the information you are working with. If you are uncertain about the sensitivity of any information or the steps you should take to secure it, ask your supervisor.

- Only use systems authorized by our Viridis Graduate Institute to store, process or transmit sensitive information. Do not copy or store sensitive information to any unauthorized systems or accounts, such as personal laptops or personal email accounts.

- If you transfer sensitive information, use secure, authorized methods that support strong encryption. Do not transfer sensitive data using insecure means, such as email, unless you are using specialized encryption software that you have been properly trained to use.

- Never store or share sensitive information on public Internet or Cloud services such as Dropbox, Apple iCloud or Google Drive unless you have prior authorization from management.

Hacked

Unfortunately, there is no simple way to determine if you are hacked. Often when your computer or your account is compromised cyber criminals take steps to make it difficult for you to find out. However, here are some things you can look for as indicators you have been hacked.

- First, your anti-virus generates an alert. Your anti-virus software should scan your computer every time you save, open or run a file.
- Second, your browser is taking you to unwanted websites or random websites open on your screen and you cannot close them. Sometimes cyber criminals will reprogram your computer to take you to websites you do not want to go.
- Third, your passwords no longer work. Cyber criminals will often change your password after hacking your account so they maintain control of it.
- Fourth, your friends or co-workers tell you they are receiving odd messages from your Facebook, Twitter or email accounts that you know you did not send.

Privacy

Technological advances have made it easier than ever before to access and share information. However, these advances have also brought tremendous responsibility. We all share a duty to help maintain the privacy of others, especially when we handle their personal information.

As part of duties at Viridis Graduate Institute, you may handle personal information such as someone's Social Security number, their financial information, their education records, or aspects of their health or medical records. You may not realize it, but there are a number of laws and regulations that require you to protect the privacy of that personal information. More importantly, you should safeguard that information out of respect for others. You should take steps to protect the privacy of people's information just as you would want them to protect the privacy of your information. Here are some steps that you can take to help protect the privacy of others:

- Limit the amount of personal information you collect, use or share.
- Only share personal information with authorized users who have a need to know.
- Store personal information only on authorized, secure systems.
- Personal information should not be kept longer than necessary. Securely archive or destroy the information when it is no longer needed.
- Understand and follow Viridis Graduate Institute's data management policies and procedures.

International Travel

Here are some key steps you should take before you travel:

- Ensure any devices you are traveling with have been secured, to include having the latest patches and updates, enabled firewall and current anti-virus.
- Learn what you can about any unique laws or regulations about the country you are visiting.
- Be sure that when you are traveling, any on-line communications are encrypted, such as when you check your email or browse online. You may be provided VPN technology for this.
- Ensure that you, your family or your friends do not post your travel plans on social media or public forums. Also disable geo-location on your mobile devices so your location while you travel is not

tracked or published.

Conclusion

Always ensure your computer, mobile devices and applications are updated and running the latest version.

Always protect Viridis Graduate Institute's confidential information. Ensure our data is securely stored and only share it with authorized people who have a need to know.

Technology is a tremendous tool that enables you to accomplish amazing things. Our goal is simply for you to leverage the latest technology while protecting yourself and Viridis Graduate Institute.

Source: Shared by University of California Santa Barbara Technical Team.

I have read and agree to the precautions and recommendations stated in the VGI Cyber Awareness Training and will follow the policies put forth by Viridis Graduate Institute.

Signature:

Print Name:

Date: